EXHIBIT L

THE RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE

Second Edition

Unabridged

THE RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE

Second Edition

Unabridged

THE RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE

Second Edition

Unabridged

Dedicated to the memory of
Jess Stein

Published in the United States by Random House, Inc., and simultaneously in Canada by Random House of Canada Limited, Toronto

Library of Congress Cataloging-in-Publication Data
The Random House dictionary of the English language.
(Random House dictionaries)
1. English language—Dictionaries. I. Flexner, Stuart Berg. II. Series.
PE1625.R3 1987 423 87-4500
ISBN 0-394-50050-4; 0-394-56500-2 deluxe ed.

other adjustment made in order to increase accuracy, as in the use of an instrument or the solution of a problem: *A five degree correction will put the ship on course.* **6.** a reversal of the trend of stock prices, esp. temporarily, as after a sharp advance or decline in the previous trading sessions. [1300–50; ME *correccio(u)n* (< AF) < L *corrēctiōn-* (s. of *corrēctiō*) a setting straight. See CORRECT, -ION]

cor•rec•tion•al (kə rek′shə nl), *adj.* of or pertaining to correction, esp. to penal correction. [1830–40; CORRECTION + -AL¹]

correc′tional facil′ity, a prison, esp. for long-term confinement. Also, **correc′tion facil′ity.** [1970–75]

correc′tional of′ficer, an officer of a jail or prison, esp. a guard. Also, **correc′tion of′ficer, correc′tions of′ficer.** [1970–75]

correc′tion flu′id, an opaque, quick-drying fluid for obliterating handwritten or typewritten matter.

cor•rect•i•tude (kə rek′ti to͞od′, -tyo͞od′), *n.* correctness, esp. of manners and conduct. [1890–95; b. CORRECT and RECTITUDE]

cor•rec•tive (kə rek′tiv), *adj.* **1.** tending to correct or rectify; remedial: *corrective exercises.* —*n.* **2.** a means of correcting; corrective agent. [1525–35; (< AF) < ML *corrēctīvus.* See CORRECT, -IVE] —**cor•rec′tive•ly,** *adv.*

correc′tor plate′, *Optics.* See **correcting plate.**

Cor•reg•gio (kə rej′ō, -rej′ē ō′; *It.* kôr red′jō), *n.* **Antonio Al•le•gri da** (än tô′nyô äl le′grē dä), 1494–1534, Italian painter.

cor•reg•i•dor (kə reg′i dôr′, -dōr′; *Sp.* kôr re′hē thôr′), *n., pl.* **-dors, -do•res** (-dôr′ēz, -dōr′-; *Sp.* -thô′res). **1.** the chief magistrate of a town in Spain. **2.** *Hist.* (in Spanish America) **a.** a minor administrative unit. **b.** the chief officer of such a district. [1585–95; < Sp. deriv. of *corregir* to CORRECT]

Cor•reg•i•dor (kə reg′i dôr′, -dōr′; *Sp.* kôr re′hē thôr′), *n.* an island in Manila Bay, in the Philippines: U.S. forces defeated by the Japanese in May, 1942. 2 sq. mi. (5 sq. km).

correl., correlative.

cor•re•late (*v., adj.* kôr′ə lāt′, kor′-; *n.* kôr′ə lit, -lāt′, kor′-), *v.,* **-lat•ed, -lat•ing,** *adj., n.* —*v.t.* **1.** to place in or bring into mutual or reciprocal relation; establish in orderly connection: *to correlate expenses and income.* —*v.i.* **2.** to have a mutual or reciprocal relation; stand in correlation: *The results of the two tests correlate to a high degree.* —*adj.* **3.** mutually or reciprocally related. —*n.* **4.** either of two related things, esp. when one implies the other. [1635–45; prob. back formation from CORRELATION and CORRELATIVE] —**cor′re•lat′a•ble,** *adj.*

cor•re•la•tion (kôr′ə lā′shən, kor′-), *n.* **1.** mutual relation of two or more things, parts, etc. **2.** the act of correlating or state of being correlated. **3.** *Statistics.* the degree to which two or more attributes or measurements on the same group of elements show a tendency to vary together. **4.** *Physiol.* the interdependence or reciprocal relations of organs or functions. **5.** *Geol.* the demonstrable equivalence, in age or lithology, of two or more stratigraphic units, as formations or members of such. Also, *esp. Brit.,* **corelation.** [1555–65; < ML *correlātiōn-* (s. of *correlātiō*). See COR-, RELATION] —**cor′re•la′tion•al,** *adj.*

correla′tion coeffi′cient, *Statistics.* one of a number of measures of correlation, usually assuming values from +1 to −1. Also called **coefficient of correlation.** [1905–10]

correla′tion ra′tio, *Statistics.* the ratio of the variance between arrays of data within a sample to the variance of the whole sample.

cor•rel•a•tive (kə rel′ə tiv), *adj.* **1.** so related that each implies or complements the other. **2.** being in correlation; mutually related. **3.** *Gram.* answering to or complementing one another and regularly used in association, as *either* and *or, not only* and *but.* **4.** *Biol.* (of a typical structure of an organism) found in correlation with another. —*n.* **5.** either of two things, as two terms, that are correlative. **6.** *Gram.* a correlative expression. Also, *esp. Brit.,* **corelative.** [1520–30; < ML *correlātīvus.* See COR-, RELATIVE] —**cor•rel′a•tive•ly,** *adv.* —**cor•rel′a•tive•ness, cor•rel′a•tiv′i•ty,** *n.*

correl′ative conjunc′tion, *Gram.* either member of a matched pair of words, of which the second is a coordinating conjunction, as *either . . . or, neither . . . nor, both . . . and,* or *not only . . . but.*

corresp., correspondence.

cor•re•spond (kôr′ə spond′, kor′-), *v.i.* **1.** to be in agreement or conformity (often fol. by *with* or *to*): *His actions do not correspond with his words.* **2.** to be similar or analogous; be equivalent in function, position, amount, etc. (usually fol. by *to*): *The U.S. Congress corresponds to the British Parliament.* **3.** to communicate by exchange of letters. [1520–30; < (< MF) ML *correspondēre.* See COR-, RESPOND] —**cor′re•spond′ing•ly,** *adv.*

—**Syn. 1.** harmonize, match, tally. CORRESPOND, AGREE, ACCORD imply comparing persons or things and finding that they harmonize. CORRESPOND suggests having an obvious similarity, though not agreeing in every detail: *Part of this report corresponds with the facts.* AGREE implies having or arriving at a condition in which no essential difference of opinion or detail is evident: *All the reports agree.* ACCORD emphasizes agreeing exactly, both in fact and in point of view: *This report accords with the other.*

cor•re•spond•ence (kôr′ə spon′dəns, kor′-), *n.* **1.** communication by exchange of letters. **2.** a letter or letters that pass between correspondents. *It will take me* ...

Correspond′ence Commit′tee. See **Committee of Correspondence.**

correspond′ence course′, a course of instruction provided by a correspondence school. [1900–05]

correspond′ence prin′ciple, *Physics.* the principle that the laws of quantum mechanics and of any new theory that may be developed reduce to the laws of Newtonian mechanics and electromagnetic theory when applied to systems in which Planck's constant can be regarded as negligible, wavelengths are comparatively small, dimensions are relatively large, etc. Also called **principle of correspondence.** [1920–25]

correspond′ence school′, a school operating on a system in which study materials and tests are mailed to the students, who in turn mail their work back to the school for grading. [1885–90]

correspond′ence the′ory, *Philos.* the theory of truth that a statement is rendered true by the existence of a fact with corresponding elements and a similar structure. Cf. **coherence theory, pragmatic theory.** [1900–05]

cor•re•spond•en•cy (kôr′ə spon′dən sē, kor′-), *n., pl.* **-cies.** correspondence (def. 3). [1580–90]

cor•re•spond•ent (kôr′ə spon′dənt, kor′-), *n.* **1.** a person who communicates by letters. **2.** a person employed by a news agency, periodical, television network, etc., to gather, report, or contribute news, articles, and the like regularly from a distant place. **3.** a person who contributes a letter or letters to a newspaper, magazine, etc. **4.** a person or firm that has regular business relations with another, esp. at a distance. **5.** a thing that corresponds to something else. —*adj.* **6.** consistent, similar, or analogous; corresponding. [1375–1425; late ME < ML *correspondent-* (s. of *correspondēns*), prp. of *correspondēre* to CORRESPOND; see -ENT] —**cor′re•spond′ent•ly,** *adv.*

correspond′ent bank′, a bank that performs services for one or more other banks. [1960–65] —**correspond′ent bank′ing.**

cor•re•spond•ing (kôr′ə spon′ding, kor′-), *adj.* **1.** identical in all essentials or respects: *corresponding fingerprints.* **2.** similar in position, purpose, form, etc.: *corresponding officials in two states.* **3.** associated in a working or other relationship: *a bolt and its corresponding nut.* **4.** dealing with correspondence: *a corresponding secretary.* **5.** employing the mails as a means of association: *a corresponding member of a club.* [1570–80; CORRESPOND + -ING²] —**cor′re•spond′ing•ly,** *adv.*

cor′respond′ing an′gles, *Geom.* two nonadjacent angles made by the crossing of two lines by a third line, one angle being interior, the other exterior, and both being on the same side of the third line. Cf. **alternate angles.** [1790–1800]

cor•re•spon•sive (kôr′ə spon′siv, kor′-), *adj.* responsive to effort or impulse; answering. [1600–10; < ML *correspons(us)* (ptp. of *correspondēre* to CORRESPOND, equiv. to *correspond-* v.s. + *-tus* ptp. suffix) + -IVE] —**cor′re•spon′sive•ly,** *adv.*

Cor•rèze (kô rez′), *n.* a department in central France. 240,363; 2273 sq. mi. (5885 sq. km). *Cap.:* Tulle.

cor•ri•da (kô rē′də; *Sp.* kôr rē′thä), *n., pl.* **-das** (-dəz; *Sp.* -thäs). a bullfight. [1895–1900; < Sp, short for *corrida de toros* lit., course, running of bulls; *corrida,* fem. of *corrido,* ptp. of *correr* < L *currere* to run]

cor•ri•do (kô rē′dō; *Sp.* kôr rē′thō), *n., pl.* **-dos** (-dōz; *Sp.* -thōs). a Mexican ballad or folksong about struggle against oppression and injustice. [< MexSp, Sp; see CORRIDA]

cor•ri•dor (kôr′i dər, -dôr′, kor′-), *n.* **1.** a gallery or passage connecting parts of a building; hallway. **2.** a passage into which several rooms or apartments open. **3.** a passageway in a passenger ship or railroad car permitting access to separate cabins or compartments. **4.** a narrow tract of land forming a passageway, as one connecting two major cities or one belonging to an inland country and affording an outlet to the sea: *the Polish Corridor.* **5.** a usually densely populated region characterized by one or more well-traveled routes used by railroad, airline, or other carriers: *The Northeast corridor extends from Washington, D.C., to Boston.* **6.** *Aeron.* a restricted path along which an aircraft must travel to avoid hostile action, other air traffic, etc. **7.** *Aerospace.* a carefully calculated path through the atmosphere along which a space vehicle must travel after launch or during reentry in order to attain a desired orbit, to avoid severe acceleration and deceleration, or to minimize aerodynamic heating. [1585–95; < MF < Upper It *corridore* (Tuscan *corridoio*), equiv. to *corr(ere)* to run (< L *currere*) + *-idore* < L *-i-tōrium;* see -I-, -TORY²] —**cor′ri•dored,** *adj.*

cor•rie (kôr′ē, kor′ē), *n. Scot.* a circular hollow in the side of a hill or mountain. [1785–95; < ScotGael *coire* cauldron, whirlpool, hollow]

Cor•rie•dale (kôr′ē dāl′, kor′-), *n.* one of a breed of sheep raised originally in New Zealand and noted for their high-quality wool and good market lambs. [1900–05; after an estate near Otago Harbor, New Zealand, where the breed was developed]

Cor•ri•en•tes (kôr′rē en′tes), *n.* a port in NE Argentina, on the Paraná River. 179,590.

Cor•ri•gan (kôr′i gən, kor′-), *n.* **Mai•read** (mə rād′), born 1944, Northern Irish peace activist: Nobel peace prize 1976.

cor•ri•gen•dum (kôr′i jen′dəm, kor′-), *n., pl.* **-da** (-də). **1.** an error to be corrected, esp. ...

corrig(ere) to CORRECT + *-ibilis* -IBLE] ...ty, **cor′ri•gi•ble•ness,** *n.* —**cor′ri•gi•b**...

cor•ri•val (kə rī′vəl), ... —*n.* **1.** a r... —*adj.* **2.** rival; competitive. [1570–80; ... joint rival. See COR-, RIVAL] —**cor•ri′v**...

cor•rob•o•rant (kə rob′ər ənt), *adj.* ... confirming. **2.** *Archaic.* strengthening; ... a medicine. —*n.* **3.** something that strengthens. **4.** *Archaic.* a strength... [1620–30; < L *corrōborant-* (s. of *corrōb*...ening, prp. of *corrōborāre.* See CORROBO...

cor•rob•o•rate (*v.* kə rob′ə rāt′; *adj.* ... **-rat•ed, -rat•ing,** *adj.* —*v.t.* **1.** to mal... confirm: *He corroborated my account* ... —*adj.* **2.** *Archaic.* confirmed. [152... *rōborātus* ptp. of *corrōborāre* to stren... *cor-* COR- + *rōbor(āre)* to make strong ... *rōbur* oak (hence, strength); see ROBUST ... —**cor•rob•o•ra•tive** (kə rob′ə rā′tiv, ... **rob′o•ra•to′ry,** *adj.* —**cor•rob′o•ra•ti**... **o•ra•to′ri•ly,** *adv.* —**cor•rob′o•ra′tor,** ... —**Syn. 1.** verify, authenticate, suppor...

cor•rob•o•ra•tion (kə rob′ə rā′shən), ... corroborating. **2.** a corroboratory fact, ... [1425–75; late ME (< MF) < LL *corrobor*... *rōborātiō*). See CORROBORATE, -ION]

cor•rob•o•ree (kə rob′ə rē), *n.* *Austra*... sembly of Aborigines typified by singi... sometimes associated with traditional sa... social gathering, esp. of a boisterous na... **rob′bo•ree.** [1793; < Dharuk *ga-ra-ba*...

cor•rode (kə rōd′), *v.,* **-rod•ed, -rod•i**... eat or wear away gradually as if by g... chemical action. **2.** to impair; deteriorat... *roded his character.* —*v.i.* **3.** to be... [1350–1400; ME (< MF) < L *corrōdere* tc... equiv. to *cor-* COR- + *rōdere* to gnaw; ... —**cor•rod′ent,** *n.* —**cor•rod′er,** *n.* ... *adj.* —**cor•rod′i•bil′i•ty,** *n.*

cor•ro•dy (kôr′ə dē, kor′-), *n., pl.* -... *Law.* corody.

cor•ro•sion (kə rō′zhən), *n.* **1.** the a... corroding; condition of being corroded. ... corroding, as rust. [1350–1400; ME (< M... *siōn-* (s. of *corrōsiō*) a gnawing away, eq... *s(us),* ptp. of *corrōdere* to CORRODE + *-iō*... **ro′sion•al,** *adj.*

cor•ro•sive (kə rō′siv), *adj.* **1.** havin... corroding or eating away; erosive. **2.** ... structive; deleterious: *the corrosive effec*... *their marriage.* **3.** sharply sarcastic; ca... *comments on the speaker's integrity.* —... corrosive, as an acid or drug. [1350–14... MF) < ML *corrōsīvus,* equiv. to L *corrōs*... SION) + *-īvus* -IVE; r. ME *corosif* < MF ... —**cor•ro′sive•ly,** *adv.* —**cor•ro′sive•ne**... **ty** (kôr′ō siv′i tē, kor′-), *n.*

corro′sive sub′limate, *Chem.* Now ... chloride. [1700–10]

cor•ru•gate (*v.* kôr′ə gāt′, kor′-; *adj.* ... kor′-), *v.,* **-gat•ed, -gat•ing,** *adj.* —*v.t.* ... bend into folds or alternate furrows an... wrinkle, as the skin or face. **3.** *Wester*... irrigation ditches in (a field). —*v.i.* **4.** to... gated; undergo corrugation. —*adj.* **5.** co... kled; furrowed. [1375–1425; late ME < ... ptp. of *corrūgāre,* equiv. to *cor-* COR- + *ri*... kle + *-ātus* -ATE¹] —**cor′ru•gat′ed,** ... **ga′tor,** *n.*

cor′rugated i′ron, a type of sheet ... strengthened for use in construction by ... of alternating grooves and ridges forced i... ally galvanized for weather resistance. [...

cor′rugated pa′per, heavy paper w... grooves, used in packing fragile articles.

cor•ru•ga•tion (kôr′ə gā′shən, kor′-), *n*... state of corrugating or of being corrugat... kle; fold; furrow; ridge. [1520–30; < ML ... of *corrūgātiō*) a wrinkling. See CORRUGAT...

cor•rupt (kə rupt′), *adj.* **1.** guilty of ... tices, as bribery; lacking integrity; croo... *judge.* **2.** debased in character; deprav... wicked; evil: *a corrupt society.* **3.** made ... rors or alterations, as a text. **4.** infecte... decayed; putrid. —*v.t.* **6.** to destroy th... cause to be dishonest, disloyal, etc., esp. ... to lower morally; pervert: *to corrupt youth*... language, text, etc.) for the worse; debas... spoil. **10.** to infect; taint. **11.** to make pu... cent. **12.** *Eng. Law.* to subject (an attain... corruption of blood. —*v.i.* **13.** to be... [1250–1300; ME (< AF) < L *corruptus* br... corrupted (ptp. of *corrumpere*), equiv. to ... *rup-* (var. s. of *rumpere* to break) + *-t* ... —**cor•rupt′ed•ly,** *adv.* —**cor•rupt′ed•ne**... **rupt′er, cor•rup′tor,** *n.* —**cor•rup′tive**... **rup′tive•ly,** *adv.* —**cor•rupt′ly,** *adv.* ... **ness,** *n.*

—**Syn. 1.** false, untrustworthy. CORRU... VENAL apply to one, esp. in public office... mercenary motives, without regard to h... justice. A CORRUPT politician is one origina... has succumbed to temptation and begu... practices. A DISHONEST politician is one ... integrity. A VENAL politician is one so tota... to sell patronage. **3, 4.** contaminated. **4.** ...

other adjustment made in order to increase accuracy, as in the use of an instrument or the solution of a problem: *A five degree correction will put the ship on course.* **6.** a reversal of the trend of stock prices, esp. temporarily, as after a sharp advance or decline in the previous trading sessions [1300–50; ME *correccio(u)n* (< AF) < L *corrēctiōn-* (s. of *corrēctiō*) a setting straight See CORRECT, -ION]

cor·rec·tion·al (kə rek′shə nl), *adj.* of or pertaining to correction, esp. to penal correction [1830–40; CORRECTION + -AL[1]]

correc′tional facil′ity, a prison, esp. for long-term confinement. Also, **correc′tion facil′ity.** [1970–75]

correc′tional of′ficer, an officer of a jail or prison, esp. a guard. Also, **correc′tion of′ficer, correc′tions of′ficer.** [1970–75]

correc′tion flu′id, an opaque, quick-drying fluid for obliterating handwritten or typewritten matter.

cor·rect·i·tude (kə rek′ti to͞od′, -tyo͞od′), *n.* correctness, esp. of manners and conduct [1890–95; b. CORRECT and RECTITUDE]

cor·rec·tive (kə rek′tiv), *adj.* **1.** tending to correct or rectify; remedial: *corrective exercises.* —*n.* **2.** a means of correcting; corrective agent. [1525–35; (< AF) < ML *corrēctīvus* See CORRECT, -IVE] —**cor·rec′tive·ly,** *adv.*

correc′tor plate′, *Optics.* See **correcting plate.**

Cor·reg·gio (kə rej′ō, -rej′ē ō′; *It.* kôr red′jô), *n.* **Antonio Al·le·gri da** (än tô′nyô äl le′grē dä), 1494–1534. Italian painter.

cor·reg·i·dor (kə reg′i dôr′, -dōr′; *Sp.* kôr ʀe′hē-thôʀ′), *n., pl.* **-dors, -do·res** (-dôr′ēz, -dōr′-; *Sp.* -thô′ʀes). **1.** the chief magistrate of a town in Spain. **2.** *Hist.* (in Spanish America) **a.** a minor administrative unit. **b.** the chief officer of such a district. [1585–95; < Sp. deriv. of *corregir* to CORRECT]

Cor·reg·i·dor (kə reg′i dôr′, -dōr′; *Sp.* kôr ʀe′hē-thôʀ′), *n.* an island in Manila Bay, in the Philippines: U.S forces defeated by the Japanese in May, 1942. 2 sq. mi (5 sq. km)

correl., correlative.

cor·re·late (*v., adj.* kôr′ə lāt′, kor′-; *n.* kôr′ə lit, -lāt′, kor′-), *v.,* **-lat·ed, -lat·ing,** *adj., n.* —*v.t.* **1.** to place in or bring into mutual or reciprocal relation; establish in orderly connection: *to correlate expenses and income.* —*v.i.* **2.** to have a mutual or reciprocal relation; stand in correlation: *The results of the two tests correlate to a high degree.* —*adj.* **3.** mutually or reciprocally related. —*n.* **4.** either of two related things, esp. when one implies the other. [1635–45; prob. back formation from CORRELATION and CORRELATIVE] —**cor′re·lat′a·ble,** *adj.*

cor·re·la·tion (kôr′ə lā′shən, kor′-), *n.* **1.** mutual relation of two or more things, parts, etc. **2.** the act of correlating or state of being correlated. **3.** *Statistics.* the degree to which two or more attributes or measurements on the same group of elements show a tendency to vary together. **4.** *Physiol.* the interdependence or reciprocal relations of organs or functions. **5.** *Geol.* the demonstrable equivalence, in age or lithology, of two or more stratigraphic units, as formations or members of such. Also, *esp. Brit.,* **corelation.** [1555–65; < ML *correlātiōn-* (s. of *correlātiō*). See COR-, RELATION] —**cor′re·la′tion·al,** *adj.*

correla′tion coeffi′cient, *Statistics.* one of a number of measures of correlation, usually assuming values from +1 to −1. Also called **coefficient of correlation.** [1905–10]

correla′tion ra′tio, *Statistics.* the ratio of the variance between arrays of data within a sample to the variance of the whole sample.

cor·rel·a·tive (kə rel′ə tiv), *adj.* **1.** so related that each implies or complements the other. **2.** being in correlation; mutually related. **3.** *Gram.* answering to or complementing one another and regularly used in association, as *either* and *or, not only* and *but.* **4.** *Biol.* (of a typical structure of an organism) found in correlation with another. —*n.* **5.** either of two things, as two terms, that are correlative. **6.** *Gram.* a correlative expression. Also, *esp. Brit.,* **corelative.** [1520–30; < ML *correlātīvus.* See COR-, RELATIVE] —**cor·rel′a·tive·ly,** *adv.* —**cor·rel′a·tive·ness, cor·rel′a·tiv′i·ty,** *n.*

correl′ative conjunc′tion, *Gram.* either member of a matched pair of words, of which the second is a coordinating conjunction, as *either ... or, neither ... nor, both ... and,* or *not only ... but.*

corresp., correspondence.

cor·re·spond (kôr′ə spond′, kor′-), *v.i.* **1.** to be in agreement or conformity (often fol. by *with* or *to*): *His actions do not correspond with his words.* **2.** to be similar or analogous; be equivalent in function, position, amount, etc. (usually fol. by *to*): *The U.S. Congress corresponds to the British Parliament.* **3.** to communicate by exchange of letters. [1520–30; < (< MF) ML *correspondēre.* See COR-, RESPOND] —**cor′re·spond′ing·ly,** *adv.*

—**Syn. 1.** harmonize, match, tally. CORRESPOND, AGREE, ACCORD imply comparing persons or things and finding that they harmonize. CORRESPOND suggests having an obvious similarity, though not agreeing in every detail: *Part of this report corresponds with the facts.* AGREE implies having or arriving at a condition in which no essential difference of opinion or detail is evident: *All the reports agree.* ACCORD emphasizes agreeing exactly, both in fact and in point of view: *This report accords with the other.*

cor·re·spond·ence (kôr′ə spon′dəns, kor′-), *n.* **1.** communication by exchange of letters. **2.** a letter or let-

Correspond′ence Commit′tee. See **Committee of Correspondence.**

correspond′ence course′, a course of instruction provided by a correspondence school. [1900–05]

correspond′ence prin′ciple, *Physics.* the principle that the laws of quantum mechanics and of any new theory that may be developed reduce to the laws of Newtonian mechanics and electromagnetic theory when applied to systems in which Planck's constant can be regarded as negligible, wavelengths are comparatively small, dimensions are relatively large, etc. Also called **principle of correspondence.** [1920–25]

correspond′ence school′, a school operating on a system in which study materials and tests are mailed to the students, who in turn mail their work back to the school for grading. [1885–90]

correspond′ence the′ory, *Philos.* the theory of truth that a statement is rendered true by the existence of a fact with corresponding elements and a similar structure. Cf. **coherence theory, pragmatic theory.** [1900–05]

cor·re·spond·en·cy (kôr′ə spon′dən sē, kor′-), *n., pl.* **-cies.** correspondence (def. 3) [1580–90]

cor·re·spond·ent (kôr′ə spon′dənt, kor′-), *n.* **1.** a person who communicates by letters. **2.** a person employed by a news agency, periodical, television network, etc., to gather, report, or contribute news, articles, and the like regularly from a distant place. **3.** a person who contributes a letter or letters to a newspaper, magazine, etc. **4.** a person or firm that has regular business relations with another, esp. at a distance. **5.** a thing that corresponds to something else. —*adj.* **6.** consistent, similar, or analogous; corresponding. [1375–1425; late ME < ML *correspondent-* (s. of *correspondēns*), prp. of *correspondēre* to CORRESPOND; see -ENT] —**cor′re·spond′ent·ly,** *adv.*

correspond′ent bank′, a bank that performs services for one or more other banks. [1960–65] —**correspond′ent bank′ing.**

cor·re·spond·ing (kôr′ə spon′ding, kor′-), *adj.* **1.** identical in all essentials or respects: *corresponding fingerprints.* **2.** similar in position, purpose, form, etc.: *corresponding officials in two states.* **3.** associated in a working or other relationship: *a bolt and its corresponding nut.* **4.** dealing with correspondence: *a corresponding secretary.* **5.** employing the mails as a means of association: *a corresponding member of a club.* [1570–80; CORRESPOND + -ING[2]] —**cor′re·spond′ing·ly,** *adv.*

cor′respond′ing an′gles, *Geom.* two nonadjacent angles made by the crossing of two lines by a third line, one angle being interior, the other exterior, and both being on the same side of the third line. Cf. **alternate angles.** [1790–1800]

cor·re·spon·sive (kôr′ə spon′siv, kor′-), *adj.* responsive to effort or impulse; answering. [1600–10; < ML *correspons(us)* (ptp. of *correspondēre* to CORRESPOND, equiv. to *correspond-* v.s. + *-tus* ptp suffix) + -IVE] —**cor′re·spon′sive·ly,** *adv.*

Cor·rèze (kô ʀez′), *n.* a department in central France. 240,363; 2273 sq. mi (5885 sq. km). *Cap.:* Tulle.

cor·ri·da (kô rē′də; *Sp.* kôʀ ʀē′thä), *n., pl.* **-das** (-dəz; *Sp.* -thäs). a bullfight. [1895–1900; < Sp. short for *corrida de toros* lit., course, running of bulls; *corrida,* fem. of *corrido,* ptp. of *correr* < L *currere* to run]

cor·ri·do (kô rē′dō; *Sp.* kôʀ ʀē′thô), *n., pl.* **-dos** (-dōz; *Sp.* -thôs). a Mexican ballad or folksong about struggle against oppression and injustice. [< MexSp, Sp; see CORRIDA]

cor·ri·dor (kôr′i dər, -dôr′, kor′-), *n.* **1.** a gallery or passage connecting parts of a building; hallway. **2.** a passage into which several rooms or apartments open. **3.** a passageway in a passenger ship or railroad car permitting access to separate cabins or compartments. **4.** a narrow tract of land forming a passageway, as one connecting two major cities or one belonging to an inland country and affording an outlet to the sea: *the Polish Corridor.* **5.** a usually densely populated region characterized by one or more well-traveled routes used by railroad, airline, or other carriers: *The Northeast corridor extends from Washington, D.C., to Boston.* **6.** *Aeron.* a restricted path along which an aircraft must travel to avoid hostile action, other air traffic, etc. **7.** *Aerospace.* a carefully calculated path through the atmosphere along which a space vehicle must travel after launch or during reentry in order to attain a desired orbit, to avoid severe acceleration and deceleration, or to minimize aerodynamic heating. [1585–95; < MF < Upper It *corridore* (Tuscan *corridoio*), equiv. to *corr(ere)* to run (< L *currere*) + *-idore* < L *-i-tōrium;* see -I-, -TORY[2]] —**cor′ri·dored,** *adj*

cor·rie (kôr′ē, kor′ē), *n. Scot.* a circular hollow in the side of a hill or mountain. [1785–95; < ScotGael *coire* cauldron, whirlpool, hollow]

Cor·rie·dale (kôr′ē dāl′, kor′-), *n.* one of a breed of sheep raised originally in New Zealand and noted for their high-quality wool and good market lambs. [1900–05; after an estate near Otago Harbor, New Zealand, where the breed was developed]

Cor·ri·en·tes (kôʀ′ʀē en′tes), *n.* a port in NE Argentina, on the Paraná River. 179,590.

Cor·ri·gan (kôr′i gən, kor′-), *n.* **Mai·read** (mə rād′), born 1944. Northern Irish peace activist: Nobel peace prize 1976.

cor·ri·gen·dum (kôr′i jen′dəm, kor′-), *n., pl.* **-da**

corrig(ere) to CORRECT + *-ibilis* -IBLE] —**cor′ ty, cor′ri·gi·ble·ness,** *n.* —**cor′ri·gi·bly,** *adv*

cor·ri·val (kə rī′vəl), —*n.* **1.** a rival; co —*adj.* **2.** rival; competitive [1570–80; < L joint rival. See COR-, RIVAL] —**cor·ri′val·ry,** *n*

cor·rob·o·rant (kə rob′ər ənt), *adj.* **1.** corr confirming. **2.** *Archaic.* strengthening; invigo a medicine. —*n.* **3.** something that corrob strengthens. **4.** *Archaic.* a strengthening [1620–30; < L *corrōborant-* (s. of *corrōborāns*) ening, prp. of *corrōborāre.* See CORROBORATE, -

cor·rob·o·rate (*v.* kə rob′ə rāt′; *adj.* kə rob -**rat·ed, -rat·ing,** *adj.* —*v.t.* **1.** to make mor confirm: *He corroborated my account of the* —*adj.* **2.** *Archaic.* confirmed. [1520–30; *rōborātus* ptp. of *corrōborāre* to strengthen, *cor-* COR- + *rōbor(āre)* to make strong (deriv *rōbur* oak (hence, strength); see ROBUST) + -at —**cor·rob·o·ra·tive** (kə rob′ə rā′tiv, -ər ə **rob′o·ra·to′ry,** *adj.* —**cor·rob′o·ra′tive·ly, o·ra·to′ri·ly,** *adv.* —**cor·rob′o·ra′tor,** *n*

—**Syn. 1.** verify, authenticate, support, valid

cor·rob·o·ra·tion (kə rob′ə rā′shən), *n.* **1.** corroborating. **2.** a corroboratory fact, stater [1425–75; late ME (< MF) < LL *corrōborātiōn- rōborātiō*) See CORROBORATE, -ION]

cor·rob·o·ree (kə rob′ə rē), *n. Australian.* sembly of Aborigines typified by singing and sometimes associated with traditional sacred ri social gathering, esp. of a boisterous nature. *rob′bo·ree.* [1793; < Dharuk *ga-ra-ba-ra* dai

cor·rode (kə rōd′), *v.,* **-rod·ed, -rod·ing.** — eat or wear away gradually as if by gnawing chemical action. **2.** to impair; deteriorate: *Jeal roded his character.* —*v.i.* **3.** to become [1350–1400; ME (< MF) < L *corrōdere* to gnaw equiv. to *cor-* COR- + *rōdere* to gnaw; akin to —**cor·rod′ent,** *n.* —**cor·rod′er,** *n.* —**cor·** *adj.* —**cor·rod′i·bil′i·ty,** *n.*

cor·ro·dy (kôr′ə dē, kor′-), *n., pl.* **-dies.** *Law.* corody.

cor·ro·sion (kə rō′zhən), *n.* **1.** the act or p corroding; condition of being corroded. **2.** a p corroding, as rust. [1350–1400; ME (< MF) < *siōn-* (s. of *corrōsiō*) a gnawing away, equiv to *s(us),* ptp. of *corrōdere* to CORRODE + *-iōn-* -ION **ro′sion·al,** *adj.*

cor·ro·sive (kə rō′siv), *adj.* **1.** having the q corroding or eating away; erosive. **2.** harmfu structive; deleterious: *the corrosive effect of p their marriage.* **3.** sharply sarcastic; caustic: *comments on the speaker's integrity.* —*n.* **4.** s corrosive, as an acid or drug. [1350–1400; lat MF) < ML *corrōsīvus,* equiv. to L *corrōs(us)* (se SION) + *-īvus* -IVE; r. ME *corosif* < MF < L —**cor·ro′sive·ly,** *adv.* —**cor·ro′sive·ness, cor ty** (kôr′ō siv′i tē, kor′-), *n.*

corro′sive sub′limate, *Chem. Now Rare.* chloride. [1700–10]

cor·ru·gate (*v.* kôr′ə gāt′, kor′-; *adj.* kôr′ə g kor′-), *v.,* **-gat·ed, -gat·ing,** *adj.* —*v.t.* **1.** to bend into folds or alternate furrows and ridge wrinkle, as the skin or face. **3.** *Western U.S.* irrigation ditches in (a field). —*v.i.* **4.** to becom gated; undergo corrugation. —*adj.* **5.** corrugat kled; furrowed. [1375–1425; late ME < L co ptp. of *corrūgāre,* equiv. to *cor-* COR- + *rūg(āre)* kle + *-ātus* -ATE[1]] —**cor′ru·gat′ed,** *adj.* — **ga′tor,** *n.*

cor′rugated i′ron, a type of sheet iron strengthened for use in construction by having of alternating grooves and ridges forced into it, ally galvanized for weather resistance. [1885–9

cor′rugated pa′per, heavy paper with ri grooves, used in packing fragile articles [1895-

cor·ru·ga·tion (kôr′ə gā′shən, kor′-), *n.* **1.** t state of corrugating or of being corrugated. **2.** kle; fold; furrow; ridge. [1520–30; < ML *corrūgi* of *corrūgātiō*) a wrinkling See CORRUGATE, -ION

cor·rupt (kə rupt′), *adj.* **1.** guilty of dishone tices, as bribery; lacking integrity; crooked: *a judge.* **2.** debased in character; depraved; pe wicked; evil: *a corrupt society.* **3.** made inferio rors or alterations, as a text. **4.** infected; tai decayed; putrid. —*v.t.* **6.** to destroy the inte cause to be dishonest, disloyal, etc., esp. by bri to lower morally; pervert: *to corrupt youth.* **8.** t language, text, etc.) for the worse; debase. **9.** spoil. **10.** to infect; taint. **11.** to make putrid o cent. **12.** *Eng. Law.* to subject (an attainted pe corruption of blood. —*v.i.* **13.** to become [1250–1300; ME (< AF) < L *corruptus* broken i corrupted (ptp. of *corrumpere*), equiv. to *cor- rup-* (var. s. of *rumpere* to break) + *-tus* ptp —**cor·rupt′ed·ly,** *adv.* —**cor·rupt′ed·ness,** *n.* **rupt′er, cor·rup′tor,** *n.* —**cor·rup′tive,** *adj.* **rup′tive·ly,** *adv.* —**cor·rupt′ly,** *adv.* —**co ness,** *n.*

—**Syn. 1.** false, untrustworthy. CORRUPT, DIS VENAL apply to one, esp. in public office, who mercenary motives, without regard to honor, r justice. A CORRUPT politician is one originally hor has succumbed to temptation and begun ques practices. A DISHONEST politician is one lackin integrity. A VENAL politician is one so totally del

intact 3. complete or whole, esp. not castrated or emasculated. 4. having the hymen unbroken; virginal [1400–50; late ME < L *intāctus* untouched, equiv. to *in*- IN-³ + *tāctus*, ptp. of *tangere* to touch] —**in·tact′ly**, *adv.* —**in·tact′ness**, *n.*
—**Syn.** 1. See **complete**.

in·tagl·io (in tal′yō, -täl′-; *It* ēn tä′lyô), *n., pl* **-tagl·ios**, *It* **-tagli** (-tä′lyē), *v.* —*n.* 1. incised carving, as opposed to carving in relief. 2. ornamentation with a figure or design sunk below the surface. 3. a gem, seal, piece of jewelry, or the like, cut with an incised or sunken design. 4. an incised or countersunk die. 5. a figure or design so produced. 6. a process in which a design, text, etc., is engraved into the surface of a plate so that when ink is applied and the excess is wiped off, ink remains in the grooves and is transferred to paper in printing, as in engraving or etching. 7. an impression or printing from such a design, engraving, etc. —*v.t.* 8. to incise or display in intaglio [1635–45; < It. deriv of *intagliare* to cut in, engrave, equiv to *in*- IN-² + *tagliare* to cut < LL *tāliāre*, deriv of L *tālea* a cutting; see TALLY]

in·take (in′tāk′), *n.* 1. the place or opening at which a fluid is taken into a channel, pipe, etc. 2. an act or instance of taking in: *an intake of oxygen.* 3. something that is taken in. 4. a quantity taken in: *an intake of 50 gallons a minute.* 5. a narrowing; contraction [1515–25; n. use of v phrase *take in*]

in′take man′ifold, a collection of tubes through which the fuel-air mixture flows from the carburetor or fuel injector to the intake valves of the cylinders of an internal-combustion engine

in′take valve′, a valve in the cylinder head of an internal-combustion engine that opens at the proper moment in the cycle to allow the fuel-air mixture to be drawn into the cylinder [1960–65]

in·tan·gi·ble (in tan′jə bəl), *adj.* 1. not tangible; incapable of being perceived by the sense of touch, as incorporeal or immaterial things; impalpable. 2. not definite or clear to the mind: *intangible arguments.* 3. (of an asset) existing only in connection with something else, as the goodwill of a business. —*n.* 4. something intangible, esp. an intangible asset: *Intangibles are hard to value.* [1630–40; < ML *intangibilis.* See IN-³, TANGIBLE] —**in·tan′gi·bil′i·ty, in·tan′gi·ble·ness,** *n.* —**in·tan′gi·bly,** *adv.*
—**Syn.** 2. vague, elusive, fleeting.

in·tar·si·a (in tär′sē ə), *n.* an art or technique of decorating a surface with inlaid patterns, esp. of wood mosaic, developed during the Renaissance. Also, **tarsia.** [1860–65; alter. (influenced by It *tarsia*) of It *intarsio,* deriv of *intarsiare* to inlay, equiv. to *in*- IN-² + *tarsiare* < Ar *tarṣī*′ an inlay, incrustation; see TARSIA] —**in·tar·si·ate** (in tär′sē āt′, -it), *adj.*

in·tar·sist (in tär′sist), *n.* a person who creates in or practices intarsia [INTARS(IA) + -IST]

in·te·ger (in′ti jər), *n.* 1. *Math.* one of the positive or negative numbers 1, 2, 3, etc., or zero. Cf. **whole number.** 2. a complete entity [1500–10; < L: untouched, hence, undivided, whole, equiv. to *in*- IN-³ + *-teg-* (comb. form of *tag-*, base of *tangere* to touch) + *-er* adj suffix]

in·te·ger vi·tae (in′te gen wē′tī; *Eng* in′ti jər vī′tē, vē′tī), *Latin.* blameless in life; innocent.

in·te·gra·ble (in′ti grə bəl), *adj. Math.* capable of being integrated, as a mathematical function or differential equation. [1720–30; INTEGR(ATE) + -ABLE] —**in′te·gra·bil′i·ty,** *n.*

in·te·gral (in′ti grəl, in teg′rəl), *adj.* 1. of, pertaining to, or belonging as a part of the whole; constituent or component: *integral parts.* 2. necessary to the completeness of the whole: *This point is integral to his plan.* 3. consisting or composed of parts that together constitute a whole. 4. entire; complete; whole: *the integral works of a writer.* 5. *Arith.* pertaining to or being an integer; not fractional. 6. *Math.* pertaining to or involving integrals. —*n.* 7. an integral whole. 8. *Math.* **a.** Also called **Riemann integral.** the numerical measure of the area bounded above by the graph of a given function, below by the *x*-axis, and on the sides by ordinates drawn at the endpoints of a specified interval; the limit, as the norm of partitions of the given interval approaches zero, of the sum of the products of the function evaluated at a point in each subinterval times the length of the subinterval. **b.** a primitive. **c.** any of several analogous quantities. Cf. **improper integral, line integral, multiple integral, surface integral.** [1545–55; < ML *integrālis.* See INTEGER, -AL¹] —**in′te·gral′i·ty,** *n.* —**in′te·gral·ly,** *adv.*
—**Syn.** 2. essential, indispensable, requisite.

in′tegral cal′culus, the branch of mathematics that deals with integrals, esp. the methods of ascertaining indefinite integrals and applying them to the solution of differential equations and the determining of areas, volumes, and lengths [1720–30]

in′tegral curve′, *Math.* a curve that is a geometric representation of a functional solution to a given differential equation.

in′tegral domain′, *Math.* a commutative ring in which the cancellation law holds true. [1935–40]

in′tegral equa′tion, *Math.* an equation in which an

CONCISE ETYMOLOGY KEY: <, descended or borrowed from; >, whence; b., blend of, blended; c., cognate with; cf., compare; deriv., derivative; equiv., equivalent; imit., imitative; obl., oblique; r., replacing; s., stem; sp., spelling, spelled; resp., respelling, respelled; trans., translation; ?, origin unknown; *, unattested; ‡, probably earlier than. See the full key inside the front cover.

in′tegral test′, *Math.* the theorem that a given infinite series converges if the function whose value at each integer is the corresponding term in the series is decreasing, tends to zero, and results in a finite number when integrated from one to infinity

in·te·grand (in′ti grand′), *n. Math.* the expression to be integrated [1895–1900; < L *integrandum,* n. use of neut. of *integrandus,* ger. of *integrāre* to INTEGRATE]

in·te·grant (in′ti grənt), *adj.* 1. making up or being a part of a whole; constituent. —*n.* 2. an integrant part. 3. a solid, rigid sheet of building material composed of several layers of the same or of different materials [1630–40; < L *integrant-* (s. of *integrāns*) prp of *integrāre* to INTEGRATE See INTEGER, -ANT]

in·te·graph (in′ti graf′, -gräf′), *n.* integrator (def. 2) [1880–85; b. INTEGRATE and -GRAPH]

in·te·grate (in′ti grāt′), *v.,* **-grat·ed, -grat·ing.** —*v.t.* 1. to bring together or incorporate (parts) into a whole. 2. to make up, combine, or complete to produce a whole or a larger unit, as parts do. 3. to unite or combine. 4. to give or cause to give equal opportunity and consideration to (a racial, religious, or ethnic group or a member of such a group): *to integrate minority groups in the school system.* 5. to combine (educational facilities, classes, and the like, previously segregated by race) into one unified system; desegregate. 6. to give or cause to give members of all races, religions, and ethnic groups an equal opportunity to belong to, be employed by, be customers of, or vote in (an organization, place of business, city, state, etc.): *to integrate a restaurant; to integrate a country club.* 7. *Math.* to find the integral of. 8. to indicate the total amount or the mean value of. —*v.i.* 9. to become integrated. 10. to meld with and become part of the dominant culture. 11. *Math.* **a.** to perform the operation of integration. **b.** to find the solution to a differential equation. [1630–40; < L *integrātus* ptp. of *integrāre* to renew, restore See INTEGER, -ATE¹] —**in′te·gra′tive,** *adj.*
—**Syn.** 2. merge, unify, fuse, mingle.

in·te·grat·ed (in′ti grā′tid), *adj.* 1. combining or coordinating separate elements so as to provide a harmonious, interrelated whole: *an integrated plot; an integrated course of study.* 2. organized or structured so that constituent units function cooperatively: *an integrated economy.* 3. having, including, or serving members of different racial, religious, and ethnic groups as equals: *an integrated school.* Cf. **segregated.** 4. *Sociol.* of or pertaining to a group or society whose members interact on the basis of commonly held norms or values. 5. *Psychol.* characterized by integration. [1580–90; INTEGRATE + -ED²]

in′tegrated bar′, *Law.* (in some states) a system of bar associations to which all lawyers are required to belong. Also called **incorporated bar.**

in′tegrated cir′cuit, *Electronics.* a circuit of transistors, resistors, and capacitors constructed on a single semiconductor wafer or chip, in which the components are interconnected to perform a given function. *Abbr.:* IC Also called **microcircuit.** [1955–60]

in′tegrated da′ta proc′essing. See **IDP.** [1960–65]

in′tegrated fire′ control′, *Mil.* an electronic system that locates and tracks a target, computes the data, and employs a weapon to destroy it

in′tegrated op′tics, an assembly of miniature optical elements of a size comparable to those used in electronic integrated circuits [1970–75]

in′tegrated pest′ man′agement, *Agric.* an ecological approach to pest management that combines understanding the causes of pest outbreaks, manipulating the crop ecosystem for pest control, and monitoring pest populations and their life cycles to determine if and when the use of pesticides is indicated. *Abbr.:* IPM

in′tegrating fac′tor, *Math.* a factor that upon multiplying a differential equation with the right-hand side equal to zero makes the equation integrable, usually by making the resulting expression an exact differential of some function [1855–60]

in·te·gra·tion (in′ti grā′shən), *n.* 1. an act or instance of combining into an integral whole. 2. an act or instance of integrating a racial, religious, or ethnic group. 3. an act or instance of integrating an organization, place of business, school, etc. 4. *Math.* the operation of finding the integral of a function or equation, esp. solving a differential equation. 5. behavior, as of an individual, that is in harmony with the environment. 6. *Psychol.* the organization of the constituent elements of the personality into a coordinated, harmonious whole. 7. *Genetics.* coadaptation (def. 2). [1610–20; INTEGRATE + -ION; cf. L *integrātiō* renewal]
—**Syn.** 1. combination, blending, fusing.

integra′tion by parts′, *Math.* a method of evaluating an integral by use of the formula, $\int u\,dv = uv - \int v\,du$.

in·te·gra·tion·ist (in′ti grā′shə nist), *n.* 1. a person who believes in, supports, or works for social integration. —*adj.* 2. pertaining to, favoring, or being conducive to social integration [1950–55; INTEGRATION + -IST]

in·te·gra·tor (in′ti grā′tər), *n.* 1. a person or thing that integrates. 2. Also called **integraph.** an instrument for performing numerical integrations [1875–80; INTEGRATE + -OR²]

in·teg·ri·ty (in teg′ri tē), *n.* 1. adherence to moral and ethical principles; soundness of moral character; honesty. 2. the state of being whole, entire, or undiminished: *to preserve the integrity of the empire.* 3. a sound, unimpaired, or perfect condition: *the integrity of a ship's*

—**Syn.** 1. cortex, involucre, involucrum

in·teg·u·men·ta·ry (in teg′yə men′tə rē), *adj.* pertaining to, or like an integument [1835–45; IN... MENT + -ARY]

in·tel·lect (in′tl ekt′), *n.* 1. the power or facu... the mind by which one knows or understands, as ... guished from that by which one feels and that by ... one wills; the understanding; the faculty of thinkin... acquiring knowledge. 2. capacity for thinking an... quiring knowledge, esp. of a high or complex order... tal capacity. 3. a particular mind or intelligence, ... a high order. 4. a person possessing a great capac... thought and knowledge. 5. minds collectively, a... number of persons or the persons themselves. ... 1400; ME < L *intellēctus,* equiv. to *intelleg(ere)* ... derstand + *-tus* suffix of v action; see INTELLIGE...
—**Syn.** 1. reason, sense, common sense, brain... **mind.**

in·tel·lec·tion (in′tl ek′shən), *n.* 1. the act... process of understanding; the exercise of the in... reasoning. 2. a particular act of the intellect. 3. ... ception or idea as the result of such an act; ... thought. [1400–50; late ME < ML *intellēction-* (s... *tellēctiō*). See INTELLECT, -ION]

in·tel·lec·tive (in′tl ek′tiv), *adj.* 1. having po... understand; intelligent; cognitive. 2. of or pertai... the intellect [1375–1425; late ME < L *intellēctīv*... INTELLECT, -IVE] —**in′tel·lec′tive·ly,** *adv.*

in·tel·lec·tu·al (in′tl ek′cho͞o əl), *adj.* 1. appea... or engaging the intellect: *intellectual pursuits.* 2... pertaining to the intellect or its use: *intellectual* ... 3. possessing or showing intellect or mental ca... esp. to a high degree: *an intellectual person.* 4. ... or developed by or relying on the intellect rathe... upon emotions or feelings; rational. 5. characteri... or suggesting a predominance of intellect: *an intel... way of speaking* —*n.* 6. a person of superior in... 7. a person who places a high value on or pursues ... of interest to the intellect or the more complex for... fields of knowledge, as aesthetic or philosophica... ters, esp. on an abstract and general level. 8. ... tremely rational person; a person who relies on i... rather than on emotions or feelings. 9. a person ... sionally engaged in mental labor, as a writer or t... 10. **intellectuals.** *Archaic.* **a.** the mental facul... things pertaining to the intellect [1350–1400; M... *intellēctuālis,* equiv to *intellēctu-,* s of *intellēc*... TELLECT + *-ālis* -AL¹] —**in′tel·lec′tu·al·ly,** *adv.* **tel·lec′tu·al·ness,** *n.*
—**Syn.** 1, 2. mental 3. See **intelligent.**

in·tel·lec·tu·al·ism (in′tl ek′cho͞o ə liz′əm), *n.* ... votion to intellectual pursuits. 2. the exercise of ... tellect. 3. excessive emphasis on abstract or inte... matters, esp. with a lack of proper considerat... emotions. 4. *Philos.* **a.** the doctrine that knowl... wholly or chiefly derived from pure reason. **b.** th... that reason is the final principle of reality. [1820-... TELLECTUAL + -ISM] —**in′tel·lec′tu·al·ist,** *n.* —... **lec′tu·al·is′tic,** *adj.* —**in′tel·lec′tu·al·is′ti·cal·**...

in·tel·lec·tu·al·i·ty (in′tl ek′cho͞o al′i tē), *n., p*... 1. the quality or state of being intellectual. 2. i... tual character or power. [1605–15; < LL *intellēct*... See INTELLECTUAL, -ITY]

in·tel·lec·tu·al·ize (in′tl ek′cho͞o ə līz′), *v.,* **-iz**... **ing.** —*v.t.* 1. to seek or consider the rational co... form of. 2. to make intellectual 3. to analyze ... thing) intellectually or rationally. 4. to ignore th... tional or psychological significance of (an action, ... dream, etc.) by an excessively intellectual or abst... planation. —*v.i.* 5. to talk or write intellectual... son; philosophize: *to intellectualize about worl... lems.* Also, *esp. Brit.,* **in′tel·lec′tu·al·ise′.** [1... INTELLECTUAL + -IZE] —**in′tel·lec′tu·al·i·za′**... —**in′tel·lec′tu·al·iz′er,** *n.*

in·tel·li·gence (in tel′i jəns), *n.* 1. capacity fo... ing, reasoning, understanding, and similar forms ... tal activity; aptitude in grasping truths, relati... facts, meanings, etc. 2. manifestation of a high ... capacity: *He writes with intelligence and wit.* 3. ... ulty of understanding. 4. knowledge of an ev... cumstance, etc., received or imparted; news; info... 5. the gathering or distribution of information, ... cret information. 6. *Govt.* **a.** information a... enemy or a potential enemy. **b.** the evaluated ... sions drawn from such information. **c.** an orga... or agency engaged in gathering such informatio... *tary intelligence; naval intelligence.* 7. interch... information: *They have been maintaining int... with foreign agents for years.* 8. *Christian Sc...* fundamental attribute of God, or infinite Mind. ... *cap.*) an intelligent being or spirit, esp. an inc... one, as an angel. [1350–1400; ME < L *intelliger*... INTELLIGENT, -ENCE]
—**Syn.** 1. See **mind.** 2. discernment, reason, aptitude, penetration —**Ant.** 2. stupidity.

intel′ligence a′gency, a government dep... charged with obtaining intelligence, or informat... for use by the armed forces. Also called **intel′**... **bu′reau, intel′ligence depart′ment, intel**... **office.** [1895–1900] —**intel′ligence a′gent.**

intel′ligence of′fice, 1. See **intelligence** ... 2. *Obs* an employment agency for the placeme... mestic help [1685–95]

intel′ligence of′ficer, a military officer res... for collecting and processing data on hostile ... weather, and terrain [1880–85]

intel′ligence quo′tient, *Psychol.* an int... test score that is obtained by dividing mental ag... reflects the age-graded level of performance as...

EXHIBIT M

THIS EXHIBIT HAS BEEN REDACTED IN ITS ENTIRETY

EXHIBIT N

MAIO

SOFT COMPUTING

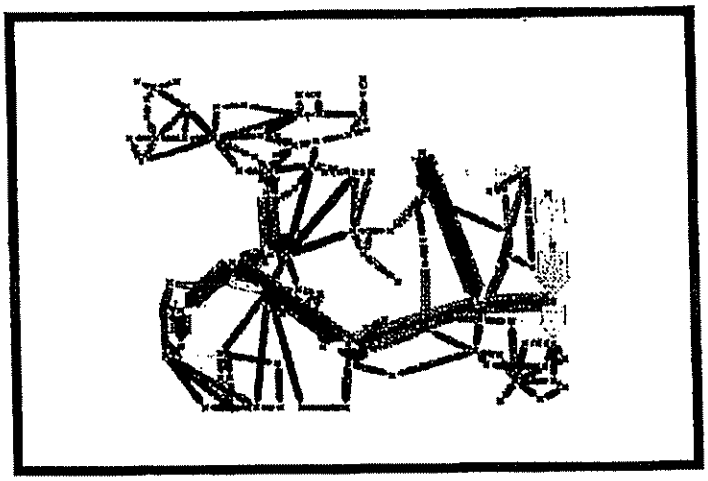
Rough Sets

Fuzzy Logic

Neural Networks

Uncertainty Management

Knowledge Discovery



Edited by
T. Y. Lin
and
A. M. Wildberger

SCS SPONSORED BY
THE SOCIETY FOR COMPUTER SIMULATION
ISBN 1-56555-077-3

Statistical Methods for Computer Usage Anomaly Detection Using NIDES (Next-Generation Intrusion Detection Expert System)

Alfonso Valdes and Debra Anderson (SRI International) January 27, 1995

Abstract : With the dramatic growth of computer networks in recent months, the need to protect the integrity of information assets from unauthorized use has never been greater. SRI's Next Generation Intrusion Detection Expert System (NIDES), a fielded system for computer system monitoring, has both an expert system component and a statistical component integrated into a client-server model and communicating to a system security officer via a window-oriented user interface. The statistical component of NIDES, NIDES/STAT, is a nonparametric anomaly detection subsystem that has been successfully used to identify suspicious behavior on the part of computer users as well as UNIX applications. NIDES/STAT learns profiles of usage behavior and then flags deviations of short-term behavior from its more slowly varying historical profiles without knowing *a priori* scenarios of computer misuse and without constructing any sort of discriminant function between subjects. Results from recent studies indicate that NIDES/STAT is quite successful in detecting abnormal patterns in application usage data.

1 Introduction

With the growing concern over security of computer systems, several organizations have developed methods to automatically detect computer usage that is possibly improper or unauthorized. One such system, SRI's NIDES (Next Generation Intrusion Detection Expert System) [1], examines audit trail information using a custom nonparametric statistical component as well as a rulebased component, and is capable of processing audit records in real time or batch mode. The statistical component, NIDES/STAT, generates an anomaly score for each audit record by comparing recent observations with a long-term or historical profile which NIDES learns for each subject. Recent observations are maintained in a short-term profile, which is an integrated summary of a subject's activity typically spanning one to a few hundred audit records (intended to reflect minutes on a typical UNIX system).

The NIDES paradigm models a computer system as a set of subjects who initiate actions that affect objects. In this paradigm explored by SRI [1, 2, 5, 6], subjects can include computer users, applications, processes, network hosts, and so forth. To date, we have successfully employed NIDES to detect anomalous use with both computer users and application programs as subjects. Herein, we present an overview of the NIDES/STAT methodology and the results of an experiment profiling UNIX applications with NIDES.

2 NIDES Statistical Algorithm Description

The statistical approach used in NIDES [3] is to compare a subject's short-term behavior with its historical or long-term behavior, considering both long-term behavior absent from short-term behavior, and short-term behavior atypical of long-term behavior. Whenever short-term behavior is sufficiently unlike long-term behavior, a warning flag is raised. In general, short-term behavior is somewhat different from long-term behavior, because short-term behavior is more concentrated on specific activities and long-term behavior is distributed across many activities. To accommodate this expected deviation, the NIDES statistical component keeps track of the amount of deviation that it has seen in the past and issues a warning only if this deviation exceeds a subject-specific threshold.

The actual processing is as follows. The statistical component receives audit data either in real time or from files. This audit data serves both to score current behavior and to train profiles, with the former operation only possible after a period of initial profile training. As each audit record is received, NIDES modifies a fading memory summary of the recent activity with the activity observed on the newly arrived record. The fading memory concept is implemented by exponential aging of various summary counts. NIDES also maintains summaries of all the activity since the last long-term profile update. The long-term profile is updated once per day in real-time operation, or when the audit data stream timestamps cross a date boundary in batch processing. Updating consists of exponential fading of the existing long-term profile and combining the summary of activity maintained since the last update.

The NIDES statistical approach requires no *a priori* knowledge about what type of behavior would result in compromised security. It simply compares short-term and long-term behaviors to determine whether they are statistically similar. This feature of the NIDES statistical component makes it ideally suited for the task of computer usage anomaly detection in the absence of intrusion scenarios.

2.1 Profile Training

NIDES describes subject behavior by means of a profile, which we separate into short-term and long-term components. Anomaly scoring compares counts in a short-term profile with expected counts (which are based on historical probabilities maintained in a long-term profile) by means of a normalized square difference measure that is computationally chi-square like in form. Aspects of subject behavior are represented as measures (characterizations of usage along such dimensions as file access, CPU usage, hour of use, and so forth). The observed difference is compared on a measure per measure basis with the empirical distribution of the historically observed difference, from which we obtain a half-normal deviate that is now comparable across all measures. The squares of these are summed and compared to historically determined thresholds.

NIDES profile training consists of three phases: NIDES first learns the historical probabilities with which various categories are observed, then NIDES learns the empirical distribution of the deviation of short-term observations about these long-term category distributions, and finally NIDES sets the score thresholds. The short-term profile changes every audit record, while the long-term profile changes at regularly scheduled profile updates. Exponential fading of both profiles (using different time constants) permits relatively compact representation of the profiles as well as a mechanism for forgetting activity from the distant past not repeated in the recent past. Exponential fading of the short-term profile takes place as each audit record is received, while fading of the long-term profile takes place at profile update time. As a consequence of this aging mechanism, we speak of effective counts when referring to a count (for example, the number of times a category has been observed) to which this aging has been applied.

NIDES uses four classes of measures: activity intensity, audit record distribution, categorical, and continuous. The activity intensity measures determine whether the volume of activity generated is normal. The audit record distribution measure determines whether, for recently observed activity, the types of actions being generated are normal. The categorical and continuous measures examine whether, within a type of activity (say, accessing a file), the types of observed categories are typical. Categorical measures are those for which the observed values are by nature categorical. For example, the file access measure would have as its categories the names of accessed files. Continuous measures are those for which the observed values are numeric, such as CPU usage. For each measure, we construct a probability distribution of short-term and long-term behaviors. For example, for the measure of file access, the long-term probability distribution would consist of the historical probabilities with which different files have been accessed, and the short-term probability distribution would consist of the recent probabilities with which different files have been accessed. In this case, the categories to which probabilities are attached are the file names. In the case of continuous measures, such as CPU time, the categories to which probabilities are attached are ranges of values, which we refer to as bins (these ranges of values are mutually exclusive and span all values from 0 to infinity). The bins are scaled multiplicatively so that the range of values is logarithmically assigned with the ratio of the first to the last bin endpoint being approximately 1000. For example, if 10 bins are available, the right endpoint of the 10th is chosen to be the data mean plus three to four standard deviations, and then each bin endpoint proceeding downward is obtained by halving the next higher. This gives a factor of ten powers of two (or 1024), as desired. The binning procedure uses fractional powers of two for any number of bins other than ten. This mechanism is sufficiently robust that the scaling parameter need not be precisely estimated. By the application of this procedure, NIDES transforms continuous measures to categorical from the standpoint of its internal computations.

Category counts and probabilities are maintained as follows. For each measure, we define the following parameters:

- H_{Neff}: historical effective n
- P_i: historical probability, category i
- $Count_i$: arithmetic count since the last long-term profile update of the number of observations of category i
- $Agecount_i$: count of observations of category i since last update, with fading
- $NCATS$: number of categories for the measure

In addition, we define the following global parameters:

- γ_s: short-term fading factor
- γ_l: long-term fading factor

We then describe the processing for each measure. Suppose that on the current audit record, category i is observed for the measure of interest. The aged and unaged counts in the short-term profile are adjusted by aging the existing counts of all categories for the measure (using the short-term aging factor) and incrementing the

count of the observed category. Algorithmically, this consists of the following steps:

$$Count_i = Count_i + 1 \ ,$$

$$Agecount_j = \gamma_s \times Agecount_j, j \neq i \ ,$$

$$Agecount_i = \gamma_s \times Agecount_i + 1 \ .$$

The *Count* field is used to modify the long-term profile at the next update interval as follows. At each update time, the counts of observations since the last long-term profile update across all categories for a given measure are totaled into "today's count" (*TodayCount* below). The historical effective n (H_{Neff}) is aged by multiplying with the long-term aging factor γ_l. The contents of the long-term profile are converted from probabilities to effective counts by multiplying each historical bin probability P_i by H_{Neff}. The counts are then combined with the counts accumulated since the last update time $Count_i$, and converted back to probabilities (dividing by the new aged count). The algorithm for the updating is outlined below:

$$TodayCount = \sum_{i=1}^{NCATS} Count_i \ ,$$

$$H_{Neff} = \gamma_l * H_{Neff} \ ,$$

$$TempCount_i = H_{Neff} \times P_i + Count_i \ ,$$

After doing the above for all categories i, the historical count is updated and the totals converted to probabilities:

$$H_{Neff} = H_{Neff} + TodayCount \ ,$$

$$P_i = TempCount_i / H_{Neff} \ .$$

After these calculations, the category probabilities are examined to see if they should be dropped or grouped into a rare class. NIDES has mechanisms for dropping categories that fall below some threshold probability and grouping as rare those categories above the drop threshold but with sufficiently small probabilities that they might affect the statistical stability of the algorithms.

2.2 Differences Between Long- and Short-term Profiles — The Q Statistic

The *Agecount* field is used for estimating the difference statistic for each audit record. The degree of difference between the long-term profile for a measure and the short-term profile for a measure is quantified using a chi-square-like statistic, with the long-term profile playing the role of the actual probability distribution and the short-term profile playing the role of the observations. We call the resultant numerical value Q; there is a different Q value for each measure, updated as each audit record is encountered. Large values of Q mean that the long-term and short-term profiles for the measure are very different from one another and therefore warrant some suspicion; a Q value of zero means that they agree exactly.

We let N_{eff} denote the short-term effective n, mathematically defined as

$$N_{eff} = \sum_{i=0}^{Nobs} \gamma_s^i \ .$$

This quantity has an asymptotic value of $\frac{1}{1-\gamma_s}$, although the algorithm uses the actual value given by the above expression. The calculation of the Q statistic proceeds as follows:

$$e_i = N_{eff} \times P_i \ ,$$

$$Q = \sum_{i=1}^{NCats} \frac{(e_i - AgeCount_i)^2}{e_i} \ .$$

The reader may note that Q is similar to a chi-square random variable. Unfortunately, it is not possible to refer Q directly to a chi-square table due to potential dependence and insufficient observations for some bins in the data stream on which Q is based. Since the distribution of Q is not chi-squared, we need to track its values to determine what its distribution looks like. We observe the values for Q (computed on each audit record) and build an empirical probability distribution for Q using an aging and updating mechanism similar to that used for the measure categories. There is a Q statistic and a corresponding Q distribution for each measure. The Q distributions look somewhat like long-tailed and stretched-out chi-square distributions. Let QP_j be the empirical probability that Q falls in bin j of its distribution, and let TP_j be the corresponding tail probability, obtained as

$$TP_j = \sum_{k=j}^{NBins} QP_k \ .$$

2.3 Scoring Anomalous Behavior – The S and $T2$ Statistic

We transform the tail probability for Q and denote the transformed variable as S, defining the transformation so that S has a half-normal distribution. (A half-normal distribution looks like the right-hand side of a normal

distribution, except that the height of the probability distribution is doubled so that there is still unit area under the curve. This is also the distribution of the absolute value of a normally distributed variable.) The mapping from tail probabilities of the Q distribution to half-normal values is obtained by interpolation from a table of the tail of a normal distribution. Mathematically, the mapping from a tail probability to an S value takes the form

$$S = \Phi^{-1}(1 - TP/2).$$

As each audit record is received, we observe the bin in the Q distribution into which the computed value of Q falls, extract the corresponding tail probability value, and generate the corresponding S value according to the above equation. This is repeated for all measures, resulting in a vector of S values. High S values correspond to measures that are unusual relative to the typical amount of discrepancy that occurs between long-term and short-term profiles. Small S values correspond to measures that are not unusual relative to the amount of discrepancy that typically occurs between long-term and short-term profiles. We combine the S scores into an overall statistic that we call $T2$. This statistic is a summary judgment of the abnormality of all active measures, and is given by the sum of the squares of the S statistics normalized by the number of measures:

$$T2 = \frac{\sum_{m=1}^{Nmeas} S_m^2}{Nmeas}.$$

As is the case with Q, we build a long-term distribution for $T2$ rather than rely on a parametric model to obtain threshold values. The long-term distribution for $T2$ is built during the last stage of the profile building period, after reasonably stable long-term distributions for the Q statistics have been constructed. We declare recent audit records to be anomalous at the yellow or warning level whenever the $T2$ value is over the 1% threshold value of the long-term empirical distribution for $T2$, and at the red or critical level whenever the $T2$ is over the 0.1% threshold.

3 Detection of Anomalous Behavior in Application Usage

SRI adapted NIDES/STAT to detect masquerading applications from exit records extracted from UNIX audit data [4]. We examined approximately three months of application use in a UNIX environment, spiked with records from two applications representing abnormal usage, with four exit records for one application and one for another. We attempted to detect these records against the trained profiles from 26 legitimate applications. We observed 101 detections in 130 opportunities, corresponding to a detection rate of approximately 77%. This is the detection rate for a single execution of a masquerading program; the probability of eventually detecting masquerader activity from several executions of the program is much higher. For example, with this detection rate, the probability of detecting at least one of two executions of a masquerading program is approximately 95%. In addition to detection performance, any system such as NIDES must also achieve an acceptably low false positive rate, defined as the percentage of detections for a subject processed through its own profile. The observed false positive rate for legitimate applications for this experiment was 1.3%, based on observations not used in the training set (the nominal false positive rate was configured to be 1%). Table 1 gives the false positive results for our experiment, as well as a summary of the detection results for the masquerader applications.

3.1 Cross-profiling Experiment

Cross profiling is the term we use when running one subject's audit data through another subject's long-term profile. In such an experiment, we use the terms host to denote the application whose profile is being used and guest to denote the application supplying the data. Cross profiling allows us to determine how unique an application's profile is and how successful other applications might be in trying to masquerade as the host application. By examining the detection rate from cross profiling we can also assess the similarity of profiles among subjects with related functionality, with an eye to constructing group profiles. Grouping may be used to provide default initial profiles for subjects based on their group membership, allowing for a faster "bootstrapping" of the NIDES profile training mechanism.

Comparing the detection rates between applications shows three possible relationships: asymmetric detection, where an application can pass through the profile of another application (a low detection rate), but the other application cannot easily pass through the profile of the original application; mutually low detection, where pairs or small groups of applications can mutually pass through each other's profiles; and mutual detection, where for a pair of applications neither can pass through the other's profile without raising suspicion.

Table 2 shows the minimum, maximum, and average detection rates using the yellow threshold (1%) for each application. Subjects with high average detection rates, such as `getfullnm` and `latex`, are very sensitive

Application Profiling Results			
	False Positive		
	Yellow	Red	Detections
as	0.0	0.0	++-+ *
cat	3.9	1.9	-** *
compile	0.0	0.0	-+* *
cp	0.0	0.0	-* *
csh	0.5	0.5	+++* *
discuss	0.7	0.0	**++ *
emacs	2.0	0.3	**++ +
finger	0.0	0.0	-+* *
fmt	0.3	0.0	+*** *
gawk	1.3	0.0	++++ *
getfullnm	2.6	1.3	**** *
ghostview	0.9	0.0	**++ *
grep	0.1	0.0	-+ *
latex	3.9	0.0	**** *
less	0.7	0.4	+++* *
ls	1.0	0.1	-* *
mail	0.0	0.0	++++ *
make	2.2	0.0	+-+ *
man	0.9	0.0	-+* *
more	0.7	0.0	-++* *
mymoreproc	0.8	0.0	+*** *
pwd	0.4	0.4	**** *
rm	0.3	0.0	-+* *
sort	1.1	0.0	-++ *
stty	0.0	0.0	++** *
vi	1.3	0.1	- *
Total *			62
Total +			39
Total -			29

This table summarizes the false-positive and detection results for the application profiling study. The false positive column shows two percents: the percent of observations above the yellow (nominally 1%) detection threshold, and the percent above the red (nominally 0.1%) threshold. The column labeled "Detections" gives the result of processing each masquerading record through the host application's profile. We have recorded an asterisk (*) for detection above the critical (red) threshold, a plus (+) for detection above the warning (yellow) threshold, and a dash (-) for no detection. The groupings indicate the results for the four instances of the first masquerader followed by the single instance of the second. At the bottom of the table are total counts of the number of red (*), yellow (+), and non-detections (-).

Table 1: Application Profiling Results

to potential masquerader data. Others, with low average rates, such as `vi` and `grep`, are more tolerant and would be candidates for a masquerading attempt. The detection thresholds for `getfullnm` and `latex` are somewhat low, while those for `vi` and `grep` are on the high side. This may explain the low detection rate for masquerader data using `vi` as a host profile and confirms our low detection rates for `vi` under our true-positive tests in the first three experiments.

	Detection Percentages(%)		
Application	Minimum	Maximum	Average
as	0.10	100	53.62
cat	0.00	98.84	52.13
compile	0.90	98.33	24.71
cp	0.00	98.77	24.07
csh	0.00	99.17	42.76
discuss	7.04	99.49	72.87
emacs	10.53	98.80	86.23
finger	3.37	99.91	59.23
fmt	34.82	100.00	90.02
gawk	14.76	100.00	75.15
getfullnm	71.54	99.98	98.24
ghostview	5.92	99.31	82.21
grep	0.00	90.94	13.38
latex	94.62	99.81	98.53
less	1.02	99.69	48.04
ls	0.00	87.87	32.84
mail	1.15	99.68	64.27
make	1.70	96.83	51.27
man	5.88	99.96	63.32
more	0.16	86.85	35.06
mymoreproc	3.29	100.00	82.40
pwd	29.64	99.74	91.82
rm	0.00	97.01	34.81
sort	6.84	99.32	82.96
stty	49.59	99.76	95.43
vi	0.00	36.97	6.19

This table shows the minimum, maximum, and average detection percents for all applications processed through the profile of the host (row) application. For example, across all subjects, the average detection rate of the as profile was 53.62%.

Table 2: Detection Results for Cross-Profiling Experiment

4 Conclusions

We have presented a summary of the NIDES statistical methodology (NIDES/STAT) and the result of using this methodology to profile UNIX applications. NIDES/STAT is embedded in SRI's NIDES, an inte-

grated system for computer anomaly detection incorporating NIDES/STAT, a rule-based component, and a graphic user interface. NIDES/STAT does not rely on parametric models or some inter-subject distance function. It learns subject behavior by observing this behavior over time, and scores new behavior according to its similarity to past behavior. The methodology does not depend on any models of inappropriate computer use. Based on recent experimental results using actual UNIX audit data, NIDES/STAT is a powerful detector, correctly classifying 77% of records representing inappropriate usage while experiencing a false positive rate of 1.3%. It is evident that NIDES/STAT can successfully detect such records as well as distinguish between legitimate subjects. The proven performance of NIDES establishes it as a leading tool for those wishing to ensure the integrity of computer systems.

Acknowledgments:

Our research was supported by the U.S. Navy who funded SRI under contract N00039-92-C-0015 and by Trusted Information Systems through contract F30602-91-C-0067 which was funded by the U.S. Air Force, Rome Laboratory.

References

[1] D. Anderson, T. Frivold, A. Tamaru, A Valdes. NIDES User Manual/Computer System Operators Manual — Beta Release. Technical Report, Computer Science Laboratory, SRI International, Menlo Park, California, June 1994.

[2] R. Jagannathan, T. F: Lunt, F. Gilham, A. Tamaru, C. Jalali, P. Neumann, D. Anderson, T. D. Garvey, and J. Lowrance. Requirements Specification: Next Generation Intrusion Detection expert system(NIDES). Technical Report, Computer Science Laboratory, SRI International, Menlo Park, California, September 1992.

[3] H. S. Javitz and A. Valdes. The NIDES Statistical Component: Description and Justification. Technical Report, Computer Science Laboratory, SRI International, Menlo Park, California, March 1994.

[4] D. Anderson, T. Lunt, H. S. Javitz, A. Tamaru, A. Valdes. Detecting Unusual Program Behavior Using the NIDES Statistical Component. Technical Rreport, Computer Science Laboratory, SRI International, Menlo Park, California, December 1993.

[5] D. Anderson, T. Frivold, A. Tamaru, A. Valdes. Next Generation Intrusion Detection Expert System (NIDES) Software Design Specifications. Technical Report, Computer Science Laboratory, SRI International, Menlo Park, California, July 1994.

[6] T. F. Lunt, Ann Tamaru, Fred Gilham, R. Jagannathan, Caveh Jalali, H. S. Javitz, A. Valdes, P. G. Neumann, and T. D. Garvey. A Real-time Intrusion Detection Expert System (IDES), Final Technical Report, Computer Science Laboratory, SRI International, Menlo Park, California, February 1992.

EXHIBIT O

Live Traffic Analysis of TCP/IP Gateways †

Phillip A. Porras
porras@csl.sri.com
Computer Science Laboratory

SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025

Alfonso Valdes
avaldes@csl.sri.com
Electromagnetic and Remote
Sensing Laboratory
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025

December 12 1997

Abstract

We enumerate a variety of ways to extend both statistical and signature-based intrusion-detection analysis techniques to monitor network traffic. Specifically, we present techniques to analyze TCP/IP packet streams that flow through network gateways for signs of malicious activity, nonmalicious failures, and other exceptional events. The intent is to demonstrate, by example, the utility of introducing gateway surveillance mechanisms to monitor network traffic. We present this discussion of gateway surveillance mechanisms as complementary to the filtering mechanisms of a large enterprise network, and illustrate the usefulness of surveillance in directly enhancing the security and stability of network operations.

1 Introduction

Mechanisms for parsing and filtering hostile external network traffic [2, 4] that could reach internal network services have become widely accepted as prerequisites for limiting the exposure of internal network assets while maintaining interconnectivity with external networks. The encoding of filtering rules for packet- or transport-layer communication should be enforced at entry points between internal networks and external traffic. Developing filtering rules that strike an optimal balance between the restrictiveness necessary to suppress the entry of unwanted traffic, while allowing the necessary flows demanded for user functionality, can be a nontrivial exercise [3].

In addition to intelligent filtering, there have been various developments in recent years in passive surveillance mechanisms to monitor network traffic for signs of malicious or anomalous (e.g., potentially erroneous) activity. Such tools attempt to provide network administrators timely insight into noteworthy exceptional activity. Real-time monitoring promises an added dimension of control and insight into the flow of traffic between the internal network and its external environment. The insight gained through fielded network traffic monitors could also aid sites in enhancing the effectiveness of their firewall filtering rules.

However, traffic monitoring is not a free activity—especially live traffic monitoring. In presenting our discussion of network analysis techniques, we fully realize the costs they imply with respect to computational resources and human oversight. For example, obtaining the necessary input for surveillance involves the deployment of instrumentation to parse, filter, and format event streams derived from potentially high-volume packet transmissions. Complex event analysis, response logic, and human management of the analysis units also introduce costs. Clearly, the introduction of network surveillance mechanisms on top of already-deployed protective traffic filters is an expense that requires justification. In this paper, we outline the benefits of our techniques and seek to persuade the reader that the costs can be worthwhile.

*† The work presented in this paper is currently funded by the Information Technology Office of the Defense Advanced Research Projects Agency, under contract number F30602-96-C-0294.

2 Toward Generalized Network Surveillance

The techniques presented in this paper are extensions of earlier work by SRI in developing analytical methods for detecting anomalous or known intrusive activity [1, 5, 12, 13]. Our earlier intrusion-detection efforts in developing IDES (Intrusion Detection Expert System) and later NIDES (Next-Generation Intrusion Detection Expert System) were oriented toward the surveillance of user-session and host-layer activity. This previous focus on session activity within host boundaries is understandable given that the primary input to intrusion-detection tools, audit data, is produced by mechanisms that tend to be locally administered within a single host or domain. However, as the importance of network security has grown, so too has the need to expand intrusion-detection technology to address network infrastructure and services. In our current research effort, EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances), we explore the extension of our intrusion-detection methods to the analysis of network activity.

Network monitoring, in the context of fault detection and diagnosis for computer network and telecommunication environments, has been studied extensively by the network management and alarm correlation community [8, 11, 15, 16]. The high-volume distributed event correlation technology promoted in some projects provides an excellent foundation for building truly scalable network-aware surveillance technology for misuse. However, these efforts focus primarily on the health and status (fault detection and/or diagnosis) or performance of the target network, and do not cover the detection of intentionally abusive traffic. Indeed, some simplifications in the fault analysis and diagnosis community (e.g., assumptions of stateless correlation, which precludes event ordering; simplistic time-out metrics for resetting the tracking of problems; ignoring individuals/sources responsible for exceptional activity) do not translate well to a malicious environment for detecting intrusions.

Earlier work in the intrusion-detection community attempting to address the issue of network surveillance includes the Network Security Monitor (NSM), developed at UC Davis [6], and the Network Anomaly Detection and Intrusion Reporter (NADIR) [7], developed at Los Alamos National Laboratory (LANL). Both performed broadcast LAN packet monitoring to analyze traffic patterns for known hostile or anomalous activity.[1] Further research by UC Davis in the Distributed Intrusion Detection System (DIDS) [23] and later Graph-based Intrusion Detection System (GRIDS) [24] projects has attempted to extend intrusion monitoring capabilities beyond LAN analysis, to provide multi-LAN and very large-scale network coverage.

This paper takes a pragmatic look at the issue of packet and/or datagram analysis based on statistical anomaly detection and signature-analysis techniques. This work is being performed in the context of SRI's latest intrusion-detection effort, EMERALD, a distributed scalable tool suite for tracking malicious activity through and across large networks [20]. EMERALD introduces a building-block approach to network surveillance, attack isolation, and automated response. The approach employs highly distributed, independently tunable, surveillance and response monitors that are deployable polymorphically at various abstract layers in a large network. These monitors demonstrate a streamlined intrusion-detection design that combines signature analysis with statistical profiling to provide localized real-time protection of the most widely used network services and components on the Internet.

Among the general types of analysis targets that EMERALD monitors are network gateways. We describe several analysis techniques that EMERALD implements, and discuss their use in analyzing malicious, faulty, and other exceptional network activity. EMERALD's surveillance modules will monitor entry points that separate external network traffic from an enterprise network and its constituent local domains.[2] We present these surveillance techniques as complementary to the filtering mechanisms of a large enterprise network, and illustrate their utility in directly enhancing the security and stability of network operations.

We first consider the candidate event streams that pass through network entry points. Critical to the effective monitoring of operations is the careful selection and organization of these event streams such that an analysis based on a selected event stream will provide meaningful insight into the target activity. We identify effective analytical techniques for processing the event stream given specific analysis objectives. Sections 4 and 5 explore how both statistical anomaly detection and signature analysis can be applied to identify activity worthy of review and possible response. All such

[1] Recent product examples, such as ASIM and Net Ranger, that follow the passive packet monitoring approach have since gained wide deployment in some Department of Defense network facilities.

[2] We use the terms *enterprise* and *intranet* interchangeably; both exist ultimately as cooperative communities of independently administered domains, communicating together with supportive network infrastructure such as firewalls, routers, and bridges.

claims are supported by examples. More broadly, in Section 6 we discuss the correlation of analysis results produced by surveillance components deployed independently throughout the entry points of our protected intranet. We discuss how events of limited significance to a local surveillance monitor may be aggregated with results from other strategically deployed monitors to provide insight into more wide-scale problems or threats against the intranet. Section 7 discusses the issue of response.

3 Event Stream Selection

The success or failure of event analysis should be quantitatively measured for qualities such as accuracy and performance: both are assessable through testing. A more difficult but equally important metric to assess is completeness. With regard to network surveillance, inaccuracy is reflected in the number of legitimate transactions flagged as abnormal or malicious (false positives), incompleteness is reflected in the number of harmful transactions that escape detection (false negatives), and performance is measured by the rate at which transactions can be processed. All three measurements of success or failure directly depend on the quality of the event stream upon which the analysis is based. Here, we consider the objective of providing real-time surveillance of TCP/IP-based networks for malicious or exceptional network traffic. In particular, our network surveillance mechanisms can be integrated onto, or interconnected with, network gateways that filter traffic between a protected intranet and external networks.

IP traffic represents an interesting candidate event stream for analysis. Individually, packets represent parsable activity records, where key data within the header and data segment can be statistically analyzed and/or heuristically parsed for response-worthy activity. However, the sheer volume of potential packets dictates careful assessment of ways to optimally organize packets into streams for efficient parsing. Thorough filtering of events and event fields such that the target activity is concisely isolated, should be applied early in the processing stage to reduce resource utilization.

With respect to TCP/IP gateway traffic monitoring, we have investigated a variety of ways to categorize and isolate groups of packets from an arbitrary packet stream. Individual packet streams can be filtered based on different isolation criteria, such as

- *Discarded traffic:* packets not allowed through the gateway because they violate filtering rules.[3]
- *Pass-through traffic:* packets allowed into the internal network from external sources.
- *Protocol-specific traffic:* packets pertaining to a common protocol as designated in the packet header. One example is the stream of all ICMP packets that reach the gateway.
- *Unassigned port traffic:* packets targeting ports to which the administrator has not assigned any network service and that also remain unblocked by the firewall.
- *Transport management messages:* packets involving transport-layer connection establishment, control, and termination (e.g., TCP SYN, RESET, ACK, <window resize>).
- *Source-address monitoring:* packets whose source addresses match well-known external sites (e.g., connections from satellite offices) or have raised suspicion from other monitoring efforts.
- *Destination-address monitoring:* all packets whose destination addresses match a given internal host or workstation.
- *Application-layer monitoring:* packets targeting a particular network service or application. This stream isolation may translate to parsing packet headers for IP/port matches (assuming an established binding between port and service) and rebuilding datagrams.

In the following sections we discuss how such traffic streams can be statistically and heuristically analyzed to provide insight into malicious and erroneous external traffic. Alternative sources of event data are also available from the report logs produced by the various gateways, firewalls, routers, and proxy-servers (e.g., router syslogs can in fact be used to collect packet information from several products). We explore how statistical and signature analysis techniques can be employed to monitor various elements within TCP/IP event streams that flow through network gateways. We present specific techniques for detecting external entities that attempt to subvert or bypass internal network services. Techniques are suggested for detecting attacks against the underlying network infrastructure, including attacks using corruption or forgery of legitimate traffic in an attempt to negatively affect routing services, application-layer services, or other network controls. We suggest

[3] Of particular added value in assessing this traffic would be some indication of why a given packet was rejected. A generic solution for deriving this *disposition* information without dependencies on the firewall or router is difficult. Such information would be a useful enhancement to packet-rejection handlers.

ISS03740

how to extend our surveillance techniques to recognize network faults and other exceptional activity. We also discuss issues of distributed result correlation.

4 Traffic Analysis with Statistical Anomaly Detection

SRI has been involved in statistical anomaly-detection research for over a decade [1, 5, 10]. Our previous work focused on the profiling of user activity through audit-trail analysis. Within the EMERALD project, we are extending the underlying statistical algorithms to profile various aspects of network traffic in search of response- or alert-worthy anomalies.

The statistical subsystem tracks subject activity via one or more variables called *measures*. The statistical algorithms employ four classes of measures: categorical, continuous, intensity, and event distribution. *Categorical* measures are those that assume values from a categorical set, such as originating host identity, destination host, and port number. *Continuous* measures are those for which observed values are numeric or ordinal, such as number of bytes transferred. Derived measures also track the intensity of activity (that is, the rate of events per unit time) and the "meta-distribution" of the measures affected by recent events. These derived measure types are referred to as *intensity* and *event distribution*.

The system we have developed maintains and updates a description of a subject's behavior with respect to these measure types in a compact, efficiently updated *profile*. The profile is subdivided into short- and long-term elements. The short-term profile accumulates values between updates, and exponentially ages values for comparison to the long-term profile. As a consequence of the aging mechanism, the short-term profile characterizes the recent activity of the subject, where "recent" is determined by the dynamically configurable aging parameters used. At update time (typically, a time of low system activity), the update function folds the short-term values observed since the last update into the long-term profile, and the short-term profile is cleared. The long-term profile is itself slowly aged to adapt to changes in subject activity. Anomaly scoring compares related attributes in the short-term profile against the long-term profile. As all evaluations are done against empirical distributions, no assumptions of parametric distributions are made, and multi-modal and categorical distributions are accommodated. Furthermore, the algorithms we have developed require no *a priori* knowledge of intrusive or exceptional activity. A more detailed mathematical description of these algorithms is given in [9, 26].

Our earlier work considered the subject class of users of a computer system and the corresponding event stream the system audit trail generated by user activity. Within the EMERALD project, we generalize these concepts so that components and software such as network gateways, proxies, and network services can themselves be made subject classes. The generated event streams are obtained from log files, packet analysis, and—where required—special-purpose instrumentation made for services of interest (e.g., FTP, HTTP, or SMTP). As appropriate, an event stream may be analyzed as a single subject, or as multiple subjects, and the same network activity can be analyzed in several ways. For example, an event stream of dropped packets permits analyses that track the reason each packet was rejected. Under such a scenario, the firewall rejecting the packet is the subject, and the measures of interest are the reason the packet was dropped (a categorical measure), and the rate of dropped packets in the recent past (one or more intensity measures tuned to time intervals of seconds to minutes). Alternatively, these dropped packets may be parsed in finer detail, supporting other analyses where the subject is, for example, the identity of the originating host.

EMERALD can also choose to separately define satellite offices and "rest of world" as different subjects for the same event stream. That is, we expect distinctions from the satellite office's use of services and access to assets to deviate widely from sessions originating from external nonaffiliated sites. Through satellite session profiling, EMERALD can monitor traffic for signs of unusual activity. In the case of the FTP service, for example, each user who gives a login name is a subject, and "anonymous" is a subject as well. Another example of a subject is the network gateway itself, in which case there is only one subject. All subjects for the same event stream (that is, all subjects within a subject class) have the same measures defined in their profiles, but the internal profile values are different.

As we migrate our statistical algorithms that had previously focused on user audit trails with users as subjects, we generalize our ability to build more abstract profiles for varied types of activity captured within our generalized notion of an event stream. In the context of statistically analyzing TCP/IP traffic streams, profiling can be derived from a variety of traffic perspectives, including profiles of

- Protocol-specific transactions (e.g., all ICMP exchanges)
- Sessions between specific internal hosts and/or spe-

cific external sites

- Application-layer-specific sessions (e.g., anonymous FTP sessions profiled individually and/or collectively)
- Discarded traffic, measuring attributes such as volume and disposition of rejections
- Connection requests, errors, and unfiltered transmission rates and disposition

Event records are generated either as a result of activity or at periodic intervals. In our case, activity records are based on the content of IP packets or transport-layer datagrams. Our event filters also construct interval summary records, which contain accumulated network traffic statistics (at a minimum, number of packets and number of kilobytes transferred). These records are constructed at the end of each interval (e.g., once per N seconds).

EMERALD's statistical algorithm adjusts its short-term profile for the measure values observed on the event record. The distribution of recently observed values is evaluated against the long-term profile, and a distance between the two is obtained. The difference is compared to a historically adaptive, subject-specific deviation. The empirical distribution of this deviation is transformed to obtain a score for the event. Anomalous events are those whose scores exceed a historically adaptive, subject-specific score threshold based on the empirical score distribution. This nonparametric approach handles all measure types and makes no assumptions on the modality of the distribution for continuous measures.

The following sections provide example scenarios of exceptional network activity that can be measured by an EMERALD statistical engine deployed to network gateways.

4.1 Categorical Measures in Network Traffic

Categorical measures assume values from a discrete, nonordered set of possibilities. Examples of categorical measures include

- Source/destination address: One expects, for example, accesses from satellite offices to originate from a set of known host identities.
- Command issued: While any single command may not in itself be anomalous, some intrusion scenarios (such as "doorknob rattling") give rise to an unusual mix of commands in the short-term profile.
- Protocol: As with commands, a single request of a given protocol may not be anomalous, but an unusual mix of protocol requests, reflected in the short-term profile, may indicate an intrusion.
- Errors and privilege violations: We track the return code from a command as a categorical measure; we expect the distribution to reflect only a small per cent of abnormal returns (the actual rate is learned in the long-term profile). While some rate of errors is normal, a high number of exceptions in the recent past is abnormal. This is reflected both in unusual frequencies for abnormal categories, detected here, and unusual count of abnormal returns, tracked as a continuous measure as described in Section 4.2.
- Malformed service requests: Categorical measures can track the occurrence of various forms of bad requests or malformed packets directed to a specific network service.
- Malformed packet disposition: Packets are dropped by a packet filter for a variety of reasons, many of which are innocuous (for example, badly formed packet header). Unusual patterns of packet rejection or error messages could lead to insight into problems in neighboring systems or more serious attempts by external sites to probe internal assets.
- File handles: Certain subjects (for example, anonymous FTP users) are restricted as to which files they can access. Attempts to access other files or to write read-only files appear anomalous Such events are often detectable by signature analysis as well.

The statistical component builds empirical distributions of the category values encountered, even if the list of possible values is open-ended, and has mechanisms for "aging out" categories whose long-term probabilities drop below a threshold.

The following is an example of categorical measures used in the surveillance of proxies for services such as SMTP or FTP. Consider a typical data-exchange sequence between an external client and an internal server within the protected network. Anonymous FTP is restricted to certain files and directories; the names of these are categories for measures pertaining to file/directory reads and (if permitted) writes. Attempted accesses to unusual directories appear anomalous. Monitors dedicated to ports include a categorical measure whose values are the protocol used. Invalid requests often lead to an access violation error; the type

ISS03742

of error associated with a request is another example of a categorical measure, and the count or rate of errors in the recent past is tracked as continuous measures, as described in Section 4.2.

4.2 Continuous Measures in Network Traffic

Continuous measures assume values from a continuous or ordinal set. Examples include inter-event time (difference in time stamps between consecutive events from the same stream), counting measures such as the number of errors of a particular type observed in the recent past, and network traffic measures (number of packets and number of kilobytes). The statistical subsystem treats continuous measures by first allocating bins appropriate to the range of values of the underlying measure, and then tracking the frequency of observation of each value range. In this way, multi-modal distributions are accommodated and much of the computational machinery used for categorical measures is shared.

Continuous measures are useful not only for intrusion detection, but also support the monitoring of health and status of the network from the perspective of connectivity and throughput. An instantaneous measure of traffic volume maintained by a gateway monitor can detect a sudden and unexpected loss in the data rate of received packets, when this volume falls outside historical norms for the gateway. This sudden drop is specific both to the gateway (the subject, in this case) and to the time of day (e.g., the average sustained traffic rate for a major network artery is much different at 11:00 a.m. than at midnight).

In our example discussion of an FTP service in Section 4.1, attempts to access unallowed directories or files result in errors. The recently observed rate of such errors is continuously compared with the rate observed over similar time spans for other FTP sessions. Some low rate of error due to misspellings or innocent attempts is to be expected, and this would be reflected in the historical profile for these measures. An excess beyond historical norms indicates anomalous activity.

Continuous measures can also work in conjunction with categorical measures to detect excessive data transfers or file uploads, or excessive mail relaying, as well as excessive service-layer errors by external clients. Categorical and continuous measures have proven to be the most useful for anomaly detection in a variety of contexts.

We next describe the two derived measure types, *intensity* and *event distribution*, which detect anomalies related to recent traffic volume and the mix of measures affected by this traffic.

4.3 Measuring Network Traffic Intensity

Intensity measures distinguish whether a given volume of traffic appears consistent with historical observations. These measures reflect the intensity of the event stream (number of events per unit time) over time intervals that are tunable. Typically, we have defined three intensity measures per profile, which, with respect to user activity monitoring, were scaled at intervals of 60 seconds, 600 seconds, and 1 hour. Applied to raw event streams, intensity measures are particularly suited for detecting flooding attacks, while also providing insight into other anomalies.

EMERALD uses volume analyses to help detect the introduction of malicious traffic, such as traffic intended to cause service denials or perform intelligence gathering, where such traffic may not necessarily be violating filtering policies. A sharp increase in the overall volume of discarded packets, as well as analysis of the disposition of the discarded packets (as discussed in Section 4.1), can provide insight into unintentionally malformed packets resulting from poor line quality or internal errors in neighboring hosts. High volumes of discarded packets can also indicate more maliciously intended transmissions such as scanning of UPD ports or IP address scanning via ICMP echoes. Excessive numbers of mail expansion requests (`EXPN`) may indicate intelligence gathering, perhaps by spammers. These and other application-layer forms of doorknob rattling can be detected by an EMERALD statistical engine when filtering is not desired.

Alternatively, a sharp increase in events viewed across longer durations may provide insight into a consistent effort to limit or prevent successful traffic flow. Intensity measures of transport-layer connection requests, such as a volume analysis of SYN-RST messages, could indicate the occurrence of a SYN-attack [17] against port availability (or possibly for port scanning). Variants of this could include intensity measures of TCP/FIN messages [14], considered a more stealthy form of port scanning.

Monitoring overall traffic volume and bursty events by using both intensity and continuous measures provides some interesting advantages over other monitoring approaches, such as user-definable heuristic rules that specify fixed thresholds. In particular, the intensity of events over a duration is relative in the sense that the term "high volume" may reasonably be considered dif-

ferent at midnight than at 11:00 a.m. The notion of high bursts of events might similarly be unique to the role of the target system in the intranet (e.g., web server host versus a user workstation). Rule developers would need to carefully define thresholds based on many factors unique to the target system. On the other hand, the statistical algorithms would, over time, build a target-specific profile that could evaluate event intensity for the given system over a variety of time slices such as the time of day (e.g., business hours versus afterhours) and/or day of the week (e.g., weekday versus weekend).

4.4 Event Distribution Measures

The event-distribution measure is a meta-measure that monitors which other measures in the profile are affected by each event. For example, an *ls* command in an FTP session affects the directory measure, but does not affect measures related to file transfer. This measure is not interesting for all event streams. For example, all network traffic event records affect the same measures (number of packets and kilobytes) defined for that event stream, so the event distribution does not change.

On the other hand, event-distribution measures are useful in correlative analysis achieved via the "Monitor of Monitors" approach. Here, each monitor contributes to an aggregate event stream for the domain of the correlation monitor. These events are generated only when the individual monitor decides that the recent behavior is anomalous (though perhaps not sufficiently anomalous by itself to trigger a declaration). Measures recorded include time stamp, monitor identifier, subject identifier, and measure identities of the most outlying measures. Overall intensity of this event stream may be indicative of a correlated attack. The distribution of which monitors and which measures are anomalous is likely to be different with an intrusion or malfunction than with the normal "innocent exception." (See Section 6 for a further discussion on result correlation.)

4.5 Statistical Session Analysis

Statistical anomaly detection via the methods described above enables EMERALD to answer questions such as how the current anonymous FTP session compares to the historical profile of all previous anonymous FTP sessions. Mail exchange could be similarly monitored for atypical exchanges (e.g., excessive mail relays).

Continuing with the example of FTP, we assign FTP-related events to a subject (the login user or "anonymous"). As several sessions may be interleaved, we maintain separate short-term profiles for each, but may score against a common long-term profile (for example, short-term profiles are maintained for each "anonymous" FTP session, but each is scored against the historical profile of "anonymous" FTP sessions). The aging mechanism in the statistics module allows it to monitor events either as the events occur or at the end of the session. We have chosen the former approach (analyze events as they happen), as it potentially detects anomalous activity in a session before that session is concluded.

5 Signature-based Network Traffic Analysis

Signature analysis is a process whereby an event stream is mapped against abstract representations of event sequences known to indicate the target activity of interest. Signature engines are essentially expert systems whose rules fire as event records are parsed that appear to indicate suspicious, if not illegal, activity. Signature rules may recognize single events that by themselves represent significant danger to the system, or they may be chained together to recognize sequences of events that represent an entire penetration scenario.

However, simplistic event to-rule binding alone does not necessarily provide enough indication to ensure accurate detection of the target activity. Signature analyses must also distinguish whether an event sequence being witnessed is actually transitioning the system into the anticipated compromised state. In addition, determining whether a given event sequence is indicative of an attack may be a function of the preconditions under which the event sequence is performed. Example coding schemes for representing operating system penetrations through audit trail analysis are [12, 18, 19].

Using basic signature-analysis concepts, EMERALD can support a variety of analyses involving packet and transport datagrams as event streams. For example, address spoofing, tunneling, source routing [21], SATAN [27] attack detection, and abuse of ICMP messages (`Redirect` and `Destination Unreachable` messages in particular) [4] could all be encoded and detected by signature engines that guard network gateways. The heuristics for analyzing headers and application datagrams for some of these abuses are not far from what is already captured by some filtering tools. In fact, it is somewhat difficult to justify the expense of passively monitoring the traffic stream for such activity when one could turn such knowledge into filtering rules.[4]

[4] On the other hand, one may also suggest a certain utility in simply having real-time mechanisms to detect, report, and hin-

Regardless, there still remain several examples that help justify the expense of employing signature analyses to monitor network traffic. In particular, there are points where the appearance of certain types of legitimate traffic introduces questions regarding the motives of the traffic source. Distinguishing benign requests from illicit ones may be fairly difficult, and such questions are ultimately site-specific. For example, EMERALD surveillance modules can encode thresholds to monitor activity such as the number of fingers, pings, or failed login requests to accounts such as guest, demo, visitor, anonymous FTP, or employees who have departed the company. Threshold analysis is a rudimentary, inexpensive technique that records the occurrence of specific events and, as the name implies, detects when the number of occurrences of that event surpasses a reasonable count.

In addition, we are developing heuristics to support the processing of application-layer transactions derived from packet monitoring. EMERALD's signature analysis module can sweep the data portion of packets in search of a variety of transactions that indicate suspicious, if not malicious, intentions by the external client. While traffic filtering rules may allow external traffic through to an internally available network service, signature analysis offers an ability to model and detect transaction requests or request parameters, alone or in combination, that are indicative of attempts to maliciously subvert or abuse the internal service. EMERALD's signature engine, for example, is capable of real-time parsing of FTP traffic through the firewall or router for unwanted transfers of configuration or specific system data, or anonymous requests to access non-public portions of the directory structure. Similarly, EMERALD can analyze anonymous FTP sessions to ensure that the file retrievals and uploads/modifications are limited to specific directories. Additionally, EMERALD's signature analysis capability is being extended to session analyses of complex and dangerous, but highly useful, services like IITTP or Gopher.

Another interesting application of signature analysis is the scanning of traffic directed at high-numbered unused ports (i.e., ports to which the administrator has not assigned a network service). Here, datagram parsing can be used to study network traffic after some threshold volume of traffic, directed at an unused port, has been exceeded. A signature module can employ a knowledge base of known telltale datagrams that are indicative of well-known network-service protocol traffic (e.g., FTP, Telnet, SMTP, HTTP). The signature module then determines whether the unknown port traffic matches any known datagram sets. Such comparisons could lead to the discovery of network services that have been installed without an administrator's knowledge.

archically correlate attempts by external sources to forward undesirable packets through a gateway.

6 Composable Surveillance of Network Traffic

The focus of surveillance need not be limited to the analysis of traffic streams through a single gateway. An extremely useful extension of anomaly detection and signature analyses is to support the hierarchical correlation of analysis results produced by multiple distributed gateway surveillance modules. Within the EMERALD framework, we are developing meta-surveillance modules that analyze the anomaly and signature reports produced by individual traffic monitors dispersed to the various entry points of external traffic into local network domains.

This concept is illustrated in Figure 1, which depicts an example enterprise network consisting of interconnected local network domains.[5] These local domains are independently administered, and could perhaps correspond to the division of computing assets among departments within commercial organizations or independent laboratories within research organizations. In this figure, connectivity with the external world is provided through one or more service providers (SP1 and SP2), which may provide a limited degree of filtering based on source address (to avoid address spoofing), as well as other primitive checks such as monitoring checksum.

Inside the perimeter of the enterprise, each local domain maintains its traffic filtering control (F-boxes) over its own subnetworks. These filters enforce domain-specific restriction over issues such as UDP port availability, as well as acceptable protocol traffic. EMERALD surveillance monitors are represented by the S-circles, and are deployed to the various entry points of the enterprise and domains.

EMERALD surveillance modules develop analysis results that are then directed up to an enterprise-layer monitor, which correlates the distributed results into a meta-event stream. The enterprise monitor is identical to the individual gateway monitors (i.e., they use the same code base), except that it is configured to correlate activity reports produced by the gateway monitors. The enterprise monitor employs both statistical anomaly detection and signature analyses to further analyze the results produced by the distributed gateway surveillance

[5] This is one example network filtering strategy that is useful for illustrating result correlation. Other strategies are possible

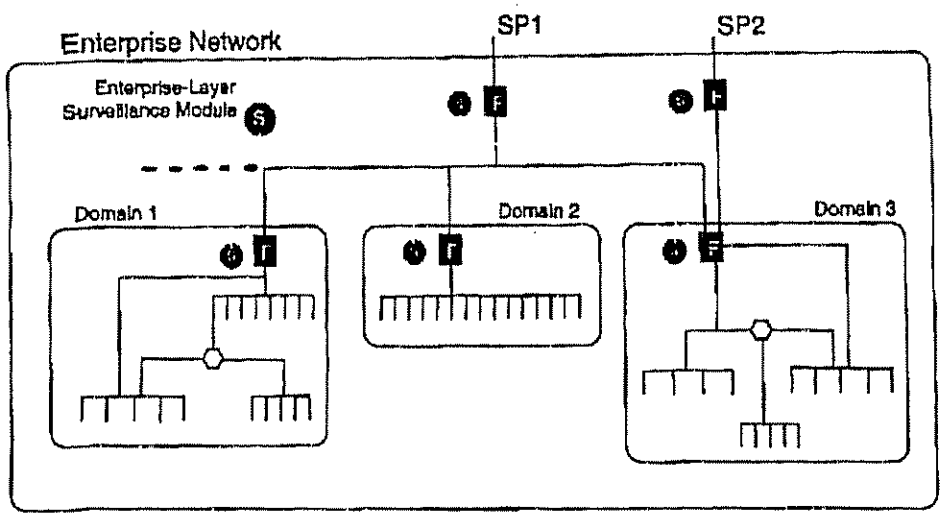


Figure 1: Example Network Deployment of Surveillance Monitors

modules, searching for commonalities or trends in the distributed analysis results.

The following sections focus on aggregate analyses that may induce both local response and/or enterprise-wide response. We enumerate some of the possible ways that analysis results from the various surveillance modules can be correlated to provide insight into more global problems not visible from the narrow perspective of local entry-point monitoring.

6.1 Commonalities among Results

One issue of direct interest is whether there exist commonalities in analysis results across surveillance modules that are examining mutually exclusive event streams. For example, a scenario previously discussed was that of a statistical engine observing a drastic increase in the number of discarded packets at the entry point to a domain, perhaps even observing the majority cause for packet discards. Depending on the degree of increase, a local domain administrator could be persuaded to take actions to help alleviate or remove the cause of the failed packets. However, if on a given day all such domains throughout the enterprise similarly observed marked increases in discarded packet volume, the response could propagate from being a local concern to being an enterprise-wide issue. Similarly, commonalities across domains in excessive levels of protocol-specific errors or signature engines detecting unwanted activity across multiple domains could lead to enterprise-layer responses

We might also choose to distinguish excessive types of certain traffic in an effort to check for intelligence gathering by outsiders who submit requests such as finger, echo, or mail alias expansion, to multiple domains in the enterprise (i.e., round-robin doorknob rattling). The objective of such a technique might be to avoid detection from both local network intensity and/or continuous measures by spreading out the probes to multiple independently monitored domains. Through aggregate analysis, we could maintain the enterprise-wide profile of probes of this type, and detect when an unusual number or mix of these probes occurs. While such probes may not appear excessive from the local domain perspective, the enterprise overall may observe a marked increase worthy of response.

In addition, we can add a layer of traffic-rate monitoring by profiling the overall volume of enterprise traffic expected throughout various slices of the day and week. Local monitors may use continuous measures to detect drastic declines in packet volumes that could indicate transmission loss or serious degradation. However, it is conceivable that the degradation from the local domain perspective, while significant, is not drastic enough to warrant active response. At the same time, we may find through results correlation that the aggregate of all domains producing reports of transmission rate degradation during the same time period could warrant attention at the enterprise layer. Thus, local domain activity below the severity of warranting a response could in

aggregation with other activity be found to warrant a response

6.2 Sequential Trend Analysis

Of general use to meta-surveillance is the modeling of activity for sequential trends in the appearance of problematic traffic. For example, this could entail correlating the analyses of local monitors, looking for trends in the propagation of application-layer datagrams for error or ICMP packets. While local responses to error messages could be handled by the local domain administrators, reports of errors spreading across all domains might more effectively be addressed by those responsible for connections between the enterprise and the service provider.

Attacks repeated against the same network service across multiple domains can also be detected through enterprise-layer correlation. For example, multiple surveillance modules deployed to various local domains in the enterprise might begin to report, in series, suspicious activity observed within sessions employing the same network service. Such reports could lead to enterprise-layer responses or warnings to other domains that have not yet experienced or reported the session anomalies. In this sense, results correlation enables the detection of spreading attacks against a common service, which first raise alarms in one domain, and gradually spread domain by domain to affect operations across the enterprise.

We are studying the use of fault-relationship models [22], in which recognition of a problem in one network component (e.g., loss of connectivity or responsiveness) could propagate as different problems in neighboring hosts (e.g., buffer overflows or connection timeout due to overloads). Our enterprise monitor employs rule-based heuristics to capture such relationship models.

7 Response Handling

Once a problem is detected, the next challenge is to formulate an effective response. In many situations, the most effective response may be no response at all, in that every response imposes some cost in system performance or (worse) human time. The extent to which a decision unit contains logic to filter out uninteresting analysis results may mean the difference between effective monitoring units and unmanageable (soon to be disabled) monitoring units. For certain analysis results such as the detection of known hostile activity through signature analyses, the necessity for response invocation may be obvious. For other analysis results such as anomaly reports, response units may require greater sophistication in the invocation logic.

Fundamental to effective response handling is the accurate identification of the source responsible for the problem. However, unlike audit-trail analysis where event-record fields such as the subject ID are produced by the OS kernel, attackers have direct control over the content and format of packet streams. Packet forgery is straightforward, and one must take care to avoid allowing attackers to manipulate response logic to harm legitimate user connectivity or cause service denials throughout the network. Some techniques have been proposed to help track network activity to the source [25].

Another issue is how to tailor a response that is appropriate given the severity of the problem, and that provides a singular effect to address the problem without harming the flow of legitimate network traffic. Countermeasures range from very passive responses, such as passive results dissemination, to highly aggressive actions, such as severing a communication channel. Within EMERALD, our response capabilities will employ the following general forms of response:

- **Passive results dissemination:** EMERALD monitors can make their analysis results available for administrative review. We are currently exploring techniques to facilitate passive dissemination of analysis results by using already-existing network protocols such as SNMP, including the translation of analysis results into an intrusion-detection management information base (MIB) structure. However, whereas it is extremely useful to integrate results dissemination into an already-existing infrastructure, we must balance this utility with the need to preserve the security and integrity of analysis results.

- **Assertive results dissemination:** Analysis results can be actively disseminated as administrative alerts. While the automatic dissemination of alerts may help to provide timely review of problems by administrators, this approach may be the most expensive form of response, in that it requires human oversight.[6]

- **Dynamic controls over logging configuration:** EMERALD monitors can perform limited

[6] Consider a network environment that on average supports 100,000 external transactions (the definition of transaction is analysis-target-specific) per day. Even if only 0.1% of the transactions were found worthy of administrative review, administrators would be asked to review 100 transactions a day.

control over the (re)configuration of logging facilities within network components (e.g., routers, firewalls, network services, audit daemons).

- **Integrity checking probes:** EMERALD monitors may invoke handlers that validate the integrity of network services or other assets. Integrity probes may be particularly useful for ensuring that privileged network services have not been subverted.[7]
- **Reverse probing:** EMERALD monitors may invoke probes in an attempt to gather as much counterintelligence about the source of suspicious traffic by using features such as *traceroute* or *finger*. However, care is required in performing such actions, as discussed in [4].
- **Active channel termination:** An EMERALD monitor can actively terminate a channel session if it detects specific known hostile activity. This is perhaps the most severe response, and care must be taken to ensure that attackers do not manipulate the surveillance monitor to deny legitimate access.

8 Conclusion

We have described event-analysis techniques developed in the intrusion detection community, and discussed their application to monitoring TCP/IP packet streams. We present a variety of exceptional activity (both malicious and nonmalicious) to which these analysis techniques could be applied. Table 1 summarizes the analyzable exceptional network activity presented in this paper, and identifies which method (statistical anomaly detection, signature analysis, or hierarchical correlation) can be utilized to detect the activity.

These examples help to justify the expense of gateway surveillance monitors, even in the presence of sophisticated traffic-filtering mechanisms. Indeed, several of the example forms of "interesting traffic" listed in Table 1 are not easily, if at all, preventable using filtering mechanisms. In addition, our surveillance modules may even help to tune or point out mistakes in filtering rules that could lead to the accidental discarding of legitimate traffic. The surveillance modules may detect the occurrence of traffic that appears to be anomalous or abusive, regardless of whether the traffic is allowed to enter, or is prevented from entering the network. Furthermore, these techniques may extend to nonmalicious problem detection such as failures in neighboring systems.

[7] A significant number of network attacks target the subversion of privileged network service. CERT Advisories CA-97.16, CA-97.12, CA-97.05 give a few recent examples.

While this paper is intended to justify and illustrate the complementary nature of combining surveillance capabilities with filtering mechanisms, in future research we will explore the practical aspects of monitor deployment, including performance analysis and secure integration into supporting network infrastructure (e.g., network management). Perhaps even more than traditional audit-based intrusion-detection developers, network monitor developers must carefully assess the optimum ways to organize and isolate the relevant traffic from which their analyses are based. The added dimension of control and insight into network operations gained by well-integrated surveillance modules is well worth consideration.

References

[1] D. Anderson, T. Frivold, and A. Valdes. Next-generation intrusion-detection expert system (NIDES): Final technical report. Technical report, Computer Science Laboratory, SRI International, Menlo Park, CA, 16 November 1994.

[2] B. Chapman and E. Zwicky. *Building internet firewalls*. O'Reilly and Associates, Inc. Sebastopol, CA, 1995.

[3] D. Chapman. Network (in)security through IP packet filtering. In *Proceedings of the Third USENIX Unix Security Symposium*, Baltimore, MD, September 1992.

[4] W.R. Cheswick and S.M. Bellovin. *Firewalls and internet security: Repelling the wily hacker*. Addison-Wesley, Reading, MA, 1994.

[5] D.E. Denning. An intrusion-detection model. *IEEE Transactions on Software Engineering*, 13(2), February 1987.

[6] L.T. Heberlein, G. Dias, K.N. Levitt, B. Mukherjee, J. Wood, and D. Wolber. A network security monitor. In *Proceedings of the 1990 Symposium on Research in Security and Privacy*, pages 296–303, Oakland, CA, May 1990. IEEE Computer Society.

[7] K. Jackson, D. DuBois, and C. Stallings. An expert system application for network intrusion detection. In *Proceedings of the Fourteenth Computer Security Group Conference*. Department of Energy, 1991.

[8] G. Jakobson and M.D. Weissman. Alarm correlation. *IEEE Network*, pages 52–59, November 1993.

ISS03748

[17] Robert T. Morris. A weakness in the 4.2bsd UNIX TCP/IP software. In *Computing Science Technical Report 117*. AT&T Bell Laboratories, Murray Hills, NJ, 25 February 1985

[18] A. Mounji, B. Le Charlier, and D. Zampunieris. Distributed audit trail analysis. In *Proceedings of the ISOC 1995 Symposium on Network and Distributed System Security*, pages 102–112, February 1995.

[19] P.A. Porras. STAT: A State Transition Analysis Tool for intrusion detection. Master's thesis, Computer Science Department, University of California, Santa Barbara, July 1992.

[20] P.A. Porras and P.G. Neumann. EMERALD: Event monitoring enabling responses to anomalous live disturbances. In *National Information Systems Security Conference*, pages 353 365, Baltimore, MD, October 1997.

[21] J. Postel. Internet protocol, request for comment, RFC 791. Technical report, Information Sciences Institute, September 1981.

[22] L. Ricciulli and N. Shacham. Modeling correlated alarms in network management systems. In *Communication Networks and Distributed Systems Modeling and Simulation*, 1997.

[23] S.R. Snapp, J. Brentano, G.V. Dias, T.L Goan, L.T. Heberlein, C.-L. Ho, K.N. Levitt, B. Mukherjee, T. Grance, D.M. Teal, and D. Mansur. DIDS (Distributed Intrusion Detection System) – motivation, architecture, and an early prototype. In *Proceedings of the Fourteenth National Computer Security Conference*, pages 167–176, Washington, D.C., 1 4 October 1991. NIST/NCSC.

[24] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, and D. Zerkle. GrIDS—a graph based intrusion detection system for large networks. In *Proceedings of the Nineteenth National Information Systems Security Conference*, pages 361–370 (Volume I), Washington D.C., October 1996. NIST/NCSC.

[25] S. Staniford-Chen and L.T. Heberlein. Holding intruders accountable on the internet. In *Proceedings of the IEEE Symposium on Security and Privacy*, 1995.

[26] A. Valdes and D. Anderson. Statistical methods for computer usage anomaly detection using NIDES. *Proceedings of the Third International Workshop on Rough Sets and Soft Computing (RSSC 94), San Jose*, January 1995.

[27] W. Venema. Project SATAN: UNIX/internet security. In *Proceedings of the COMPSEC-95 Conference*, Elsevier, London, 1995.